LEGALMAPS | LEGALKAIZEN SECURITY POLICY

Policy & Procedure Summary

Document Name	Information Security Policy		
Type:	*Policy*	**LegalMaps Policy No.**	*1.0*
Policy Owner:	LegalMaps / LegalKaizen	**Issued By:**	Security / Jeff Horton
Approved By:	Rich Young	**Prepared By:**	Jeff Horton
Effective Date	9/13/2019		
Next Review Date:	As needed		

Version Control

Date	Name	Version	Description of Changes
8/27/19	Jeff Horton	1.0	DRAFT
9/13/19	Rich Young	1.0	FINAL

Table of Contents

Information is an asset, which like other important business assets has value to an organization and consequently needs to be suitably protected. LegalMaps Security protects information from a wide range of threats in order to provide business continuity, minimize business damage and maximize return on investments and business opportunities. Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Information should always be appropriately protected regardless of the form in which it is shared or stored.

LegalMaps Security is characterized as the preservation of:

Confidentiality: Securing information so that it is accessible only to those authorized to have access;

Integrity: Safeguarding the accuracy and completeness of information and processing methods;

Availability: Providing authorized users with access to information and associated assets when required.

Security is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organizational structures, and software functions. These controls need to be established so that the specific security objectives of the organization are met.

The Security Policy is to be adopted by every user, business unit and functional area that operates under the LegalMaps brand. This policy supports a common security language through its use of ISO 27001 operating directives and covers all aspects of business operation, not just computing and Information Technology.

Regulatory Compliance

The Security Policy has been analyzed against regulatory security requirements and every reasonable effort has been made to maintain compliance. Compliance is not guaranteed and must be analyzed separately if the information system meets the criteria of any externally-imposed regulation or standard.

There are many externally-imposed information security standards that may affect information security requirements. Some of these external standards are described in Appendix A, *Relevant Laws, Regulations and Standards*. Additional external standards may be identified in the future, as new LegalMaps business activities are established or as LegalMaps engages in new business activities that are subject to existing standards. As applicable external standards are identified, they will be incorporated into this LegalMaps Security Policy.

Purpose

The LegalMaps policy for Security is designed to protect and preserve the security, confidentiality, integrity, and availability of information owned by or in the care of LegalMaps and to establish standards for a secure computing environment.

It is the policy of LegalMaps to require all information technology functions, facilities, and resources be designed, built, and operated in such a way such that the technology assets and information of LegalMaps and its customers are protected from unauthorized use, access, disclosure, modification, destruction, damage, delay, or removal, either intentional or accidental.

Intended Audience

This policy applies to all employees, contractors, temporary employees, consultants, and authorized agents of LegalMaps. Throughout this policy, the word "Users" will be used to collectively refer to all such individuals.

This policy also applies to all computer and communication systems owned by LegalMaps and its subsidiaries and affiliates whether located on LegalMaps premises or at off-site locations. Throughout this policy, the word “LegalMaps” will be used to collectively refer to LegalMaps and its subsidiaries and affiliates. This policy supersedes all other LegalMaps security related policies.

The implementation of these policies is the responsibility of all LegalMaps users. All users are required to understand the basic requirements necessary to perform their duties in a compliant manner.

Managers and technical users will need to understand this policy to best implement the technical controls and processes they will be asked to implement and the rules they will need to convey to the users of the information systems.

Policy Violations

Information, information systems, and technology are critical components of LegalMaps business. All LegalMaps users must maintain the security, confidentiality, availability, and integrity of these resources. Violations of this policy may be considered serious breaches of trust, which can result in disciplinary action up to and including termination of employment or contract and prosecution in accordance with applicable federal, state, and local laws.

Terms and Definitions

For the purposes of this document, the following definitions apply:

Information System

Information System refers to any data, information, material, or documents that provide value to LegalMaps for the purpose of conducting business activities.

Most Restrictive

The term “most restrictive” in relation to LegalMaps Security policies is defined as any statement, or statements, that are reasonably determined to be more limiting in nature, requiring an additional or advanced set of controls in relation to conflicting policy statements with an end result being a reduced level of associated risk.

Organizational Business Unit or Business Unit

An entity of a corporation that is logically, physically, or geographically separated, imposes its own management infrastructure, and holds responsibility for all assets within such entity. A Business Unit (also sometimes known as an Organizational Business Unit) as referred to within this policy could be a corporate office, subsidiary, or any functional operating unit owned and operated as a part of the parent corporation.

Risk Assessment

A risk assessment is the process used for identifying threats to and vulnerabilities of a system and the potential cost impact that the loss of information or capabilities of a system would have on LegalMaps, and using the analysis as a basis for identifying and selecting appropriate and cost-effective measures.

Revision Control

This policy will become effective upon approval by the Chief Executive Officer and will be reviewed annually to determine its effectiveness.

Documentation Format

This document has been separated into several chapters based on their relevancy to the ISO 27001 framework.

1 Scope

Each LegalMaps Business Unit that maintains an Information System with connectivity to a public or private network shall establish administrative, technical, and physical safeguards, to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, or inconvenience to LegalMaps or any individual on whom information is maintained. All resources belonging to or used by LegalMaps shall be protected at a level commensurate with the risk and magnitude of harm that could result from loss, misuse, or unauthorized access to that resource.

This LegalMaps Security Policy has been developed to aid the process of implementing and enforcing security practices for all LegalMaps Information Systems. This policy is applicable to all LegalMaps employees, contractors, temporary employees, consultants, and authorized agents of LegalMaps, offices, cafes, functional operating units, and subsidiaries. It provides policy and guidance on all aspects of security for the protection of information technology resources including roles and responsibilities, physical and logical controls, and address type and frequency of security assessment controls. It further defines responsibilities for the implementation and oversight of the policy contained herein.

2 LegalMaps Security Policy

The LegalMaps policy for LegalMaps Security is designed to protect and preserve the security, confidentiality, integrity, and availability of information owned by or in the care of LegalMaps and its subsidiaries and affiliates. All LegalMaps personnel shall protect information and assets at a level commensurate with their value.

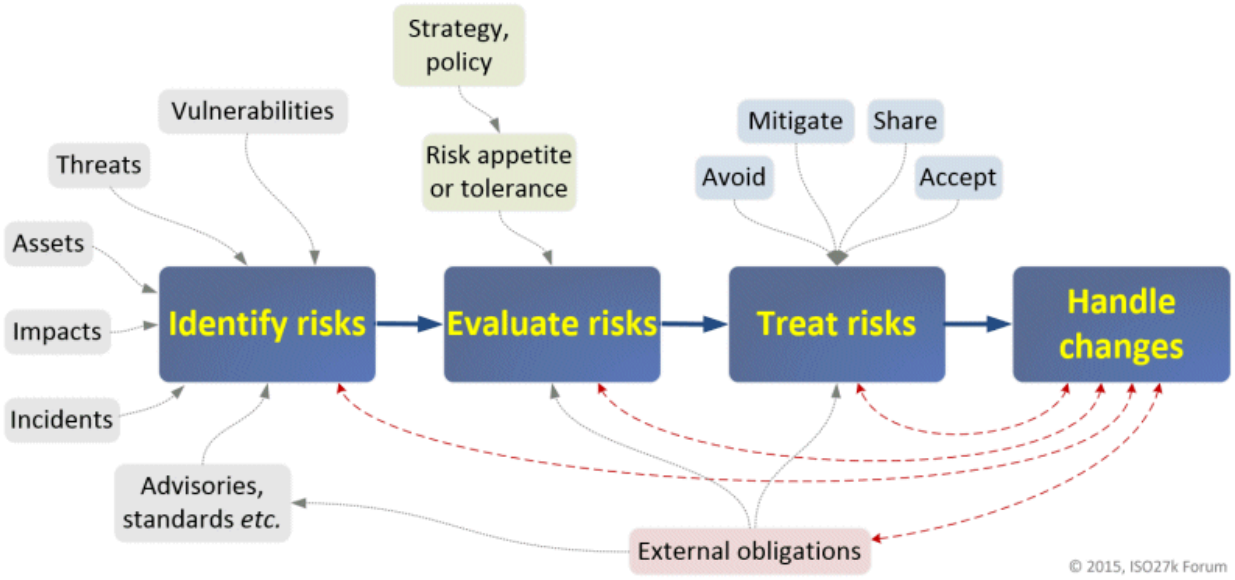
Information and Information Systems are valuable assets to LegalMaps. There is a reliance on information and Information Systems to maintain and advance the corporation's competitive edge. Security is an essential component in sustaining consumer and customer confidence and supporting LegalMaps' existing information services. Through policies, procedures, and controls, LegalMaps seeks to maintain the continued high standards for integrity, confidentiality, and availability of its resources.

2.1 LegalMaps Security Risk Assessment

The LegalMaps Security Program is based on the following policy that employs Risk Assessments to allow for simplified security control verification and enforcement. By relying on information classification, risk valuation, and security review processes, the process to apply policy requirements to a system or business process has been greatly simplified.

A formal risk assessment must be completed for all new and existing systems, applications, and third parties with whom we share consumer, customer or LegalMaps information. Security Risk Assessments are performed based on a LegalMaps approved methodology.

Diagram 2.1 Risk Assessment Methodology



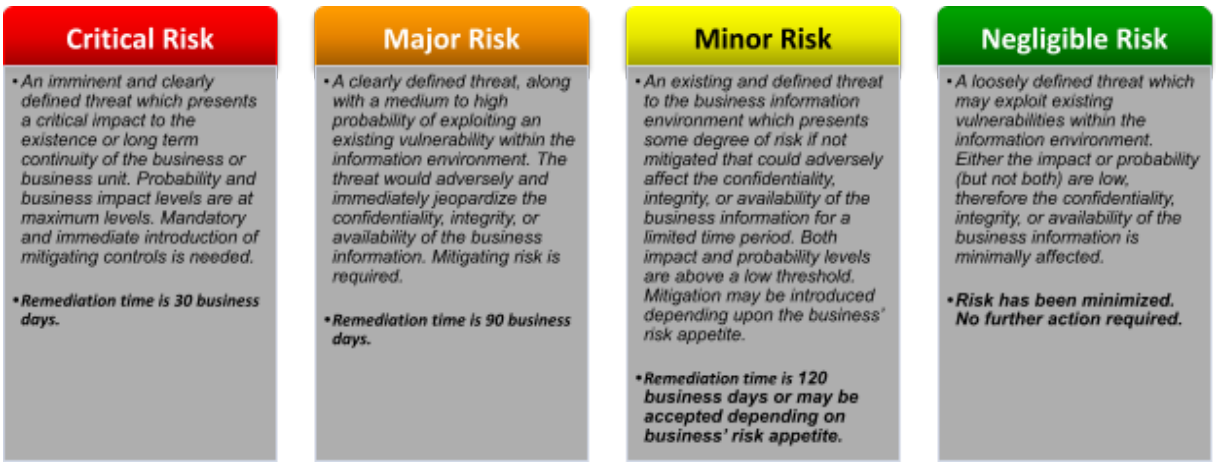
A Risk Assessment to be performed as necessary in the following circumstances:

- Deployment of a new system, application, or technology process;
- Significant changes to existing systems such as new core functionality, new data sources, new input/output mechanisms or feeder systems, changes to security tables and mechanisms, migration to a different operating system or database, a material change to the user population, or expansion of the system to new areas or departments;
- Significant alteration of the purpose or nature of the output or product of a system;
- New and deployed systems that use, capture, manipulate, transmit, or store customer information or sensitive LegalMaps data;
- Systems that use information that, if disclosed to unauthorized individuals, could damage LegalMaps' reputation or could cause financial loss to LegalMaps;
- New or renewing outside vendor data processing arrangements or
- Any use of external network connections or connections to the Internet

The Risk Assessment will determine the business risk rating. Information security risk is a product of threats in the business and technical environments that exploit existing vulnerabilities contained therein. Essential to understanding risk and enforcing remediation is determining the probability of those risks occurring within the same environment as well as the estimated costs associated with rectifying damages sustained by those threats.

Risk has varying levels, some of which the business may choose to accept, others where they may choose to mitigate, and yet other risks where remediation needs to occur based upon the estimated damage that it may cause to LegalMaps or a business unit. The risk descriptions below reflect the levels of risk that are used to collectively represent the effects of existing threat levels and vulnerabilities within the assessed environment and their levels of exposure. The risk levels have been approved by the Legal Center of Excellence and are defined as follows:

Diagram 2.2 Risk Categorization



Existing Risk Assessments will be validated on a periodic basis as determined by LegalMaps.

Requiring Risk Assessment documentation prior to an Information System going into production supports the need for system owners to document all systems and processes for inventory and assessment purposes. It also helps to illustrate that the system meets security policy requirements and that LegalMaps staff has reviewed and approved the Information System prior to internal or external exposure of potentially sensitive information.

Once the Risk Assessment documentation has been completed by the System owner and approved by LegalMaps staff, it serves as a baseline for production operations and security enforcement. By defining a classification to the information held or processed and combining it with appropriate risk valuations, LegalMaps and system owners can easily apply the appropriate security controls based on levels of classification by and, in most cases, referring to simple charts separating requirements by information classification levels.

2.1.1 Risk Assessment Requirements

Planning security into the development process requires that Risk Assessments be treated as a living document, to be updated, revised and reviewed throughout the systems development/production life cycle. The following additional requirements apply to security planning:

- All LegalMaps Information Systems are required to be documented and certified through the Risk Assessment process. It may be necessary to utilize Risk Assessment to identify the classification and risks of an Information System for purposes of security audit or to enhance existing security controls without incurring a significant modification.
- New projects involving development of Information Systems and applications must complete Risk Assessment documentation throughout the systems development life cycle with assistance from LegalMaps staff.
- Production activities may not commence until Risk Assessment documentation has been completed, reviewed by LegalMaps Security, and authorized to process in writing.
- Risk Assessment documentation will be reviewed on a routine basis or as systems changes dictate.

2.2 LegalMaps Security Policy

It is the policy of LegalMaps to require that all information technology functions, facilities, and resources be designed, built, and operated in such a way that the technology assets and information of LegalMaps and its customers are protected from unauthorized use, access, disclosure, modification, destruction, damage, delay, or removal, either intentional or accidental.

Security controls shall be employed on all media where information is stored, the systems that process it, and infrastructure components that facilitate its transmission. Controls shall be in place to restrict access to information based on the requester's need-to-know in performance of his/her official duties. Security will be incorporated into the design of software products. Known or suspected vulnerabilities or suspicious activities will be reported when detected.

2.2.1 LegalMaps Security Policy Document

LegalMaps Security is established under the guidance of the LegalMaps CEO. LegalMaps Security will establish, manage, and maintain the LegalMaps Information Security Program and report on its measurements and metrics.

This LegalMaps Security Policy document will be used by LegalMaps and relies on risk assessment, enforcement, and education such that appropriate administrative, technical, and physical safeguards are present and effective in the LegalMaps operational environment. This LegalMaps Security Policy document is designed to provide for the confidentiality of information, protect against any anticipated and unanticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to LegalMaps, its customers, or the individuals to whom the information relates.

2.2.2 LegalMaps Security Policy Review

LegalMaps Security Policy review and approval are the primary responsibility of the person responsible for Information Security, although anyone may suggest modifications at any time.

Policies may be ratified at any time but must be reviewed and accepted by the CEO with associated assignment of policy number(s) and the effective date of publication. Suggestions for policy additions or modifications should be submitted to LegalMaps Security Compliance.

Diagram 2.4

Policy Maintenance Life Cycle

Policy development, maintenance and enforcement is a continuing cycle that coincides with cross education of not only LegalMaps management and staff, but also the policy developers that must take input from management and staff directly affected by policy and ever changing technology.

At least annually, the following must be determined during policy review:

Securi

- The policy's effectiveness, demonstrated by the nature, number and impact of recorded security incidents, exceptions, and approvals;
- Cost and impact of controls on business efficiency;
- Effects of changes to technology; and
- Changing laws and regulations particular to the country in which the Information Systems reside.

2.2.2.1 Reviewing System Security Controls

LegalMaps staff will conduct security reviews, assessments, or evaluations on an Information System. These reviews may evaluate the security of the total system or a logical segment/subsystem.

2.2.3 Conflicting Policies

This policy is to serve as the overriding LegalMaps Security policy for LegalMaps and all its business units, subsidiaries, and affiliates. There may be additional policies applicable to specific business units, functions, or processes, but no other policies are to supersede the LegalMaps Security Policy.

2.2.4 Exceptions to Policy, Procedures, & Standards

Under certain circumstances, users or processes will need to employ/deploy systems that are not compliant with these policies. Approval of the Policy Exception will make it incumbent on the person(s) responsible for the system or network to take necessary programmatic, planning, and funding steps regarding implementation of any security requirements that are temporarily postponed as a consequence of approval of the Policy Exception.

The person(s) responsible for the system or network is to document and present Policy Exceptions to Security Compliance for approval on all security Exception requests.

2.2.4.1 LegalMaps Security Exception Request

Requests for a LegalMaps Security Exception must include the following on the approved Exception Request Form (an example of which can be found in LegalMaps Security Standards document):

- A statement of the requirements that are to be expected and for what duration of time;
- Name of the source policy document and citation of the policy section(s) that cannot be met;
- Evidence stating why the identified requirements cannot be implemented per policy or standard, describe the effects of the requirement on current and proposed operations, and the specific operational and technical difficulties that will result from complying with the requirement and the impact on LegalMaps;
- A well defined overview that outlines any security risks, vulnerabilities, and anticipated threats that might be created by granting the exception;
- Evidence to show that the consequent risk to the system and sensitive information it processes, stores, or transmits will be accepted based on other countermeasures that will be employed over the specified period;
- The offsetting countermeasures that will be utilized, i.e. mitigating controls; and
- A plan for bringing the Policy Exception into compliance within the appropriate timeframe determined by the Exception process.

2.2.4.2 Information System Owner for a LegalMaps Security Exception Request

The Information System Owner shall be responsible for ensuring that appropriate steps are taken to implement exceptions to security requirement(s) including details of future remediation.

2.2.4.3 Risk Review of Security Exception Requests

All Policy Exceptions must be reviewed for risk by LegalMaps Security Compliance prior to final approval.

2.2.4.4 Approval of LegalMaps Security Exceptions

Exceptions to the LegalMaps policies, procedures, and standards must be approved by the Director of Information Security or their delegates.

3 Internal Organizational Security

3.1 LegalMaps Security

The purpose of LegalMaps Security is to provide for the protection of LegalMaps information and resources in accordance with appropriate security policies, controls and applicable regulatory doctrine. Protection of LegalMaps assets is defined as;

1. Maintaining the availability of information and resources when demanded by the business and its customers;
2. Providing for the integrity of LegalMaps data; and
3. Maintaining the confidentiality of data through strong methods of authorization and on a 'need to know' and 'least privilege' basis.

LegalMaps Security encompasses the following: Security Engineering, Security Operations, Security Compliance, and Identity and access management. These disciplines provide execution surrounding policies, standards, guidelines, awareness and procedures for the protection and compliance of information processed, stored, and transmitted. These disciplines take a risk based and balanced approach to LegalMaps Security and ownership for the implementation of security best practices across the global LegalMaps enterprise.

LegalMaps Security is directed by the Director of Information Security which leads the vision, mission, objectives, and services delivered to LegalMaps to maintain the security posture of information and resources across the global LegalMaps enterprise.

3.1.1 Security Engineering Services

LegalMaps Security provides an enterprise-wide Security Engineering function that serves as a framework for the application of a consistent and unified approach by which LegalMaps operating divisions may develop and improve security within their business operations.

Security Engineering is a strategic function of understanding and subsequently balancing business risk with the appropriate strategic security initiative or solution. Security Engineering seeks to frame problems and improve operations in a way that consider both innovative solutions and the ability to execute upon emerging solutions or technologies. Core to a Security Engineering function is the ability to reduce project risk while improving productivity and quality in operations. Security Engineering seeks to develop and translate requirements into functional design specifications. Our Security Engineering professionals balance the needs of business processes, people, and technology criteria to maximize the effectiveness of solutions.

The service delivery charter for Security Engineering consists of the following:

- Advisement for IT and Key Business Initiatives
- Security Assessment and Penetration Testing Services
- Security Requirements Gathering and Design
- Security Technology Life Cycle Management
- Security Monitoring Architecture & Design
- Information Security Strategic Planning
- Internet Security Design
- Systems Security Design
- Host Security & Hardening Procedures
- Encryption & Cryptographic Standards
- Firewall Design and Configuration
- Secure Provisioning Design & Architecture
- Intrusion Prevention/Detection Design
- Network/LAN Security Design
- Security technology standards (in conjunction with LegalMaps IT teams, where necessary)

3.1.2 Security Operations

LegalMaps Security runs and maintains the LegalMaps Security tool sets implemented throughout the LegalMaps enterprise. In addition, it provides operational security support to each business division as required. Security Operations is responsible for maintaining specific expertise in all security operations so they can technically lead the day to day activities and maintenance of security solutions throughout the organization. Security Operations personnel deliver a scope of services centered on the immediate response, business support, and day to day delivery of service to the business enterprise.

Security Operations oversees the deployment, implementation, and service delivery of strategic security initiatives as designed by the Security Engineering team. This expertise is utilized internally to enable the LegalMaps business to develop an enhanced infrastructure that provides monitoring, testing, maintenance, day-to-day infrastructure operation and platform specific support.

The global service delivery charter for Security Operations consists of the following:

- Security Monitoring Center
- Desktop AV & HIPS Governance
- Intrusion Prevention System Management
- Firewall Change Management
- Data Loss Prevention

3.1.3 Security Compliance

Security Compliance services focus on understanding country, industry, regulatory, and business requirements for development of the proper policies, standards, and directives for LegalMaps. Security Compliance translates these requirements to construct the proper balance and translation to drive 'ways of acting' (controls) that support LegalMaps compliance. Key to Security Compliance is the capability to deliver strong processes for testing periodic compliance and reporting results to management. Risk assessment and analysis activities are developed and delivered by the Security Compliance team.

Policy development activities reside within Security Compliance. These directives must be cognizant of the various industry, governmental and regulatory requirements that drive our policy formulation. Standards are more detailed and should articulate ways of implementing and complying with a policy. Practices take the form of accepted, effective, and well recognized steps, procedures, tools, or products to utilize in accordance with a policy or standard.

Within Security Compliance is a clear understanding of ISO 27001 and security standards that are key to the ongoing development and management of our security policies. Standards such as PCI, Sarbanes Oxley (SOX), and those of other regulatory bodies are essential to understand.

The global service delivery charter for Security Compliance consists of the following:

- Information Security Policy & Standards Management
- Maintain the Security Awareness Program
- Risk Assessment Services
- Third Party Security Reviews
- Legal and Regulatory Compliance (SOX, PCI and Breach notification, etc.)
- Manage and Maintain Key Control Documentation
- Interface with Internal & External Audit Teams to Coordinate and Respond to Audit Requirements
- Manage External Certification Processes (PCI, SOX, etc.)

3.1.4 Physical Security

Physical Security provides for the protection of LegalMaps personnel and assets. Physical Security implements controls to mitigate the known and unknown threat posed by inside and outside risks.

Physical Security assesses, plans for, manages, implements, monitors and investigates those aspects of physical risk, for all LegalMaps property, users and assets from unauthorized access, loss, damage, assault or civil disorder or other criminal acts. Property is defined as all property, and facilities owned, leased, designed and built by, otherwise occupied or controlled by LegalMaps, its subsidiaries and affiliates.

The service delivery charter for Physical Security consists of the following:

- Oversee Physical Access Controls
- Lead or Assist with Emergency Response
- Mitigate known risks to People, Property, Proprietary Information and Corporate Image
- Protect People and Assets
- Establish Global Physical Security Policies, Standards and Guidelines
- Integrate Physical Security Systems and Programs with other Security initiatives

3.1.5 Investigations

Investigations provides support to LegalMaps' efforts to protect LegalMaps data by leveraging technology and automated processes in the LegalMaps infrastructure to stop the unauthorized or accidental change or loss of LegalMaps data. Investigations & Credentialing is responsible for all investigations, both internal and external, that involve the suspected or known compromise or misuse of LegalMaps data.

The global service delivery charter for Investigations consists of the following:

- Protect LegalMaps data by leveraging technology & automated processes
- Review & investigate cyber crimes
- Serve as a law enforcement liaison
- Investigate potential misuse of LegalMaps data
    - Security Policy Awareness
    - Customer Compliance
    - Security Contract Review
    - Physical Security
    - Security technology deployments
- Meet with key clients in support of compliance and sales activities as necessary
- Monitor legal and regulatory changes that impact security operations in conjunction with local legal counsel
- Be directly involved in the investigation and resolution of security events and assist with disciplinary and legal matters associated with such events

3.1.6 Management Commitment

LegalMaps has shown its support and commitment for enterprise security by appointing a Director of Information Security, who reports to the office of the Chief Information Officer (CIO).

3.1.7 LegalMaps Security Coordination

LegalMaps Security coordination occurs through the LegalMaps Security Compliance. The Compliance Group is a cross-functional team of security representatives from relevant parts of the organization, necessary to coordinate the implementation of LegalMaps Security controls. The LegalMaps Security Compliance is responsible for the following:

- Overseeing specific methodologies and processes for LegalMaps Security, e.g. risk assessment, security classification system;
- Supporting organization wide LegalMaps Security initiatives, e.g. Security Awareness program, security planning, etc.;
- Supporting efforts to maintain security as part of the enterprise planning process;
- Reviewing the adequacy and coordinating the implementation of specific LegalMaps Security controls for new systems or services that affect multiple operating business units;
- Reviewing Exceptions and Approvals to LegalMaps Policies and Standards as necessary;
- Reviewing Security incidents as necessary;
- Reviewing and approving LegalMaps Security policy and overall responsibilities;
- Monitoring significant changes in the exposure of resources to major threats; and
- Promoting the visibility of LegalMaps Security throughout the organization.

3.1.8 Partner Organizations Within LegalMaps

LegalMaps Security works closely with other organizations within LegalMaps to achieve the security goals and objectives for the company.

Business Continuity (BCP) and Disaster Recovery (DR)
The BCP and DR team is part of the LegalMaps Security organization and is responsible for the development and maintenance of a business continuity, crisis management, and disaster recovery program. The team coordinates data center threat and risk assessments, business impact analysis, DR/BCP strategy development, DR/BCP plan development, testing and maintenance. Regular tests of the DR and BCP plans are organized and conducted by this team. BCP and DR also work with the crisis management program and team.

3.2 Allocation of Roles and Responsibilities

LegalMaps Security is responsible for establishing and maintaining enterprise wide security policies that are reasonably designed to meet the protective needs of LegalMaps and that comply with all applicable laws and regulations. LegalMaps Security also collaborates with other functional teams within LegalMaps to establish and manage security standards, guidelines, and procedures. The focus of these activities is on LegalMaps information and customer information, regardless of the form it takes, the technology used to handle it, where it resides, the processes by which it is handled, or who possesses it. This includes consideration of the security, confidentiality, integrity, and availability of both information and the systems that handle it. While responsibility for Information Systems security on a day-to-day basis is every user's duty, specific governing authority for security is vested in LegalMaps Security.

The LegalMaps Security program will be adjusted in light of any relevant changes in technology, legal requirements, the sensitivity of its customer information and internal or external threats to information.

LegalMaps Security will, at its own discretion, directly manage or delegate certain aspects of the LegalMaps Security program to qualified areas within LegalMaps Security or its agents. In cases where such authority has been delegated, LegalMaps Security will maintain governing authority.

The responsibilities and accountability of owners, providers, and users of LegalMaps Information Systems and other parties concerned with the security of computer systems are explicit. The assignment of responsibilities may be internal to a Business Unit or extend across organizational boundaries. At the program level, responsibilities should be specifically assigned to those organizational elements and officials responsible for the implementation and continuity of the LegalMaps Security Policy.

3.2.1 Security Management

Security must be applied at the management level of all organizational business units. Thus, all business units must integrate the following responsibilities into their management structure:

- Security planning, review, and enforcement;
- Assignment of LegalMaps Security Roles and Responsibilities;
- Coordinate Security Implementation and Consult in Project Design;
- Develop and Maintain Security Processes and Procedures;
- Interact with Human Resources and Legal Departments on personnel and contractual matters;
- Develop/Administer Violations Process with the LegalMaps Security, Human Resources, and Legal departments;

Departmental managers are responsible for providing that appropriate computer and communication system security measures are observed in their area. Departmental managers are also responsible for making sure all users are aware of LegalMaps policies related to computer and communication system security.

3.2.2 Director of Information Security

The Director of Information Security (or other responsible employee) will handles the following functions:

- Providing for documentation and maintenance of security policies and standards;
- Making decisions on whether to accept the adequacy and associated risks of security controls for Information Systems;
- Confirming that the LegalMaps Security Policy is reviewed at least annually;
- Reviewing and accepting LegalMaps LegalMaps Security Policies;
- Confirming that LegalMaps effectively implements and maintains LegalMaps Security policies, procedures, and control techniques;
- Assigning members of their functional or operational unit's management the responsibility to direct LegalMaps Security activities to provide for compliance with LegalMaps policies; and
- Serving as the point of contact for security policy, implementation, and monitoring.

The Director of Information Security (or other responsible employee) will assist the Senior Leadership Team with:

- Assessing the LegalMaps Security risks associated with the operations and assets for programs and systems over which such officials have control;
- Determining the levels of LegalMaps Security appropriate to protect such operations and assets;
- Periodically testing and evaluating LegalMaps Security controls and techniques; and
- Evaluating the effectiveness of the LegalMaps Security policy; including testing control techniques and implementing appropriate remedial actions as a result of the evaluation.

3.2.3 Managers/Supervisors of System Users

Managers and supervisors are responsible for enforcing the requirement that their users read, understand, and comply with the LegalMaps Security Policy, standards, and procedures. Managers and supervisors are also responsible for promptly initiating corrective action for non-compliance with LegalMaps Security policies and standards and for notifying LegalMaps Security of security violations. Managers may also serve in the Information System Owner role. Managers at all levels are responsible for the actions of their subordinates on the system(s) for which they are authorized access. Managers of system users are responsible for the following:

- Making sure that users acknowledge they understand the system security requirements, system security rules, and their responsibilities prior to them being granted system access;
- Using LegalMaps approved medium/process to authorize access to LegalMaps systems;
- Confirming that users' access to a system is restricted to the minimum (least privilege) necessary to perform their job;
- Making sure that duties and responsibilities in critical functions are divided/separated among different individuals and that no individual has the authority or system access which could result in a fraudulent activity;
- Provide prompt notification to system's system/security administrator of changes in user status (e.g., user changes assignments and/or manager, leaves LegalMaps), and take prompt and appropriate action to change user access profile and/or remove user from the system;
- Review audit trails and reports as deemed necessary by LegalMaps Security.

3.2.4 System Users

Users, as defined in the scope of this policy as LegalMaps employees, contractors, temporary employees, consultants, and authorized agents of LegalMaps, are responsible for complying with the LegalMaps Security Policy, standards, and procedures and for reporting all LegalMaps Security violations and problems to LegalMaps Security in a timely manner.

3.2.5 Information System Owners

An Information System Owner is identified by LegalMaps Security and is the individual responsible for LegalMaps customer, financial, operational, or other data and/or the application used to access the data that is associated with a specified business function. Typically, an Information System Owner is a senior business or operations manager.

The Information System Owner is responsible for data classification decisions and security procedures that provide for the application or system complying with applicable LegalMaps Security policies and standards.

3.2.6 Control Related Organizations

LegalMaps utilizes a variety of internal and external organizations such that proper controls, including LegalMaps Security controls, are in place throughout LegalMaps. Among these organizations are Internal Audit, external auditors, and regulators. These organizations may utilize this policy to evaluate the effectiveness of controls as they pertain to LegalMaps Security.

3.2.7 Human Resources

LegalMaps staff will conduct background screening on all LegalMaps personnel as a preventive assurance against improper activities executed by users. Human Resources also works with management to determine appropriate disciplinary actions associated with policy violations.

A thorough review of an individual's background provides useful information in determining whether or not a candidate is suitable for certain functions requiring more trust, responsibility, and access to various areas of the organization. Dependent upon the position to be performed at LegalMaps, all personnel are subject to any of the following pre-screening techniques where applicable by country:

- Drug Screening: Determines whether or not drug use is part of the individual's life, which may undermine their performance within the LegalMaps environment.
- Criminal Background and Credit Checks: Recent criminal activity may indicate that trustworthiness and proper business ethics may be vulnerable to fraudulent activity.
- Professional Reference Check: Verification of prior employment and obtaining reference checks serves to validate character and work experience, as manifested by the user. Descriptive qualitative information may be obtained from this technique.
- Ongoing screening: The aforementioned background screening techniques should be continued, along with others when and where needed, at management's discretion, when determining the reliability of an existing user in managing and operating additional or separate functions to their existing line of work. Separately, management should reserve the right to conduct such on-going checks when and if probable cause exists. This should be clearly made clear to all users upon hiring.

For locations outside the US, please contact Human Resources for the latest policy.

3.2.8 Corporate Legal Resources

Corporate Legal resources are responsible for interpreting and answering questions concerning legally related issues, reviewing and preparing necessary contracts, and assisting with interpretation of laws and regulations.

3.2.9 Corporate Communications

Corporate Communications is responsible for reviewing and authorizing any communications to the media or public Information Systems in connection with LegalMaps.

3.2.10 Security Compliance Risk Assessment Services

The Risk Assessment Services department is an internal group to Security Compliance dedicated to providing Information Systems security assessments and risk analysis. The Risk Assessment department must determine the security posture of an Information System while remaining neutral to the design, maintenance and implementation of such systems. The Risk Assessment department utilizes advanced tools, techniques and methodologies that are considered more technically detailed in nature than their Corporate IT Audit counterparts and are subsequently separated in function. Risk Assessment is responsible for:

- Assessing the security of corporate Information Systems in relation to policy requirements by means of technical analysis as an independent third party to the LegalMaps Security Organization.
- Reporting system and application vulnerabilities with mitigating recommendations to asset owners in a timely manner.
- Incident reporting in accordance with policy requirements as necessary.

- Assisting in investigations as required.

3.2.11 Physical Security

LegalMaps Asset Protection is responsible for developing physical security controls. Asset Protection is responsible for, but not limited to, physical access, central computer installation, backup facilities and office environments. See Section 6 *Physical and Environmental Security* for additional details.

Asset Protection must approve all facilities containing operational corporate systems and must maintain an up-to-date inventory of all approved facilities. Only approved facilities can be used to house operational corporate systems.

3.2.12 Authorization Process for Information Processing Facilities

A management authorization process is required for new information processing facilities. The following controls are required:

- New facilities must have management approval authorizing and documenting their purpose and use.
- Approval must also be obtained through security planning documentation and acceptance from LegalMaps Security.
- The use of personal information processing facilities (ex. home offices or other facilities not deemed appropriate by LegalMaps Security for processing of corporate information) for processing business information is prohibited.

3.2.13 Confidentiality & Non-Disclosure Agreement

3.2.13.1 LegalMaps employees, consultants, contractors, and temporary personnel are required to sign a system use/confidentiality agreement before accessing any of LegalMaps' resources.

3.2.13.2 Sensitive information (Class 3 and above, see Section 4.3.3 *Information Classification Guidelines* for more details on classifications) must not be shared with any third party unless an LegalMaps approved non-disclosure agreement is in place.

3.2.13.3 No user shall sign, on behalf of LegalMaps, a non-disclosure agreement presented by a third party without prior appropriate Legal review and approval.

3.2.14 Contact with Authorities

Disclosure of information to any law enforcement authority without LegalMaps Legal Counsel is strictly prohibited. LegalMaps Investigations & Credentialing, in conjunction with Legal Counsel, will cooperate with law enforcement authorities where applicable and disclose information required for possible prosecution of LegalMaps employees, consultants, contractors, temporary personnel, third party vendors, clients, or customers using LegalMaps assets or information for illegal purposes such as, but not limited to, fraud, child pornography, etc.

3.2.15 Contact with Special Interest Groups

Appropriate contacts with special interest groups or other specialist security forums and professional associations such as CERT, NIST, NSA, SANS, etc. should be maintained and supported.

Membership in special interest groups and forums should be considered as a means to:

- Improve knowledge about the best practices and staying up to date with relevant security information;
- Provide for the understanding of the security environment is current and complete;
- Receive early warnings of alerts, advisories, and patches pertaining to attacks and vulnerabilities;
- Share and exchange information about new technologies, products, threats, or vulnerabilities;
- Provide suitable liaison points when dealing with security incidents.

3.2.16 Independent Review of LegalMaps Security

The LegalMaps Security Policy sets out the policy and responsibilities for LegalMaps Security. Its implementation should be reviewed independently to provide assurance that organizational practices properly reflect the policy, and that it is feasible and effective.

Such a review may be carried out by the internal audit function, an independent manager or a third party organization specializing in such reviews, where these candidates have the appropriate skills and experience.

3.3 External Parties

Coordination or cooperation with external organizations may be necessary or desired at certain times to assist security or business tasks. It is the responsibility of LegalMaps Security to enforce the requirement that appropriate contacts are maintained, with external groups or individuals, which may be valuable in assisting with security tasks. Maintaining those contacts is also the responsibility of LegalMaps Security. External security organizations include, but are not limited to, law enforcement agencies, security and investigation organizations, regulatory bodies and groups, professional security associations, data service providers, telecommunication service providers, etc.

3.3.1 Identification of Risk Related to External Parties

LegalMaps is committed to the security and privacy of consumer and customer information. If a product or service related to an external party is being considered for implementation in or interfacing with the LegalMaps technology environment, a risk assessment must be completed by Security Compliance.

The purpose of the risk assessment is to obtain information required to assess the third party's' internal information security and business continuity posture. Detailed and complete answers to LegalMaps' questions must be given. The completed risk assessment is the first step in assessing a third party as a potential service provider to LegalMaps. A detailed security review of the product or service may become necessary as our business relationship progresses.

3.3.1.1 Periodic Review of Adequacy of Controls

LegalMaps Security will periodically review the adequacy of third party security controls such that LegalMaps information is properly secured. The frequency of these reviews will be based on criticality and risk.

3.3.2 Security when Dealing with Customers and Consumers

Due care must be taken when speaking or interacting with customers or consumers. To protect the privacy of customers and consumers, users will:

- Not communicate or otherwise reveal customer or sensitive LegalMaps information to any third party or individual unless specifically authorized via their job function or the user has been authorized by management to release such information and the user has taken reasonable steps to verify the identity of the receiving party and their authority to receive such information;

- Not communicate or release to them or their agent, customer's or consumer's information unless reasonable steps have been taken to verify the identity of the customer or agent and the authority of the agent to receive such information. For example, account information should not be given to the customer over the phone without having taken steps to identify the customer. In the case of the customer's attorney or accountant requesting account information, steps must be taken to verify their identity and to validate their authority to receive the information on behalf of the customer.
- Not communicate LegalMaps information without a legitimate business purpose or forward information in a manner that violates the originator's desire to restrict further dissemination. Examples include, but are not limited to, confidential Human Resource data, information pertaining to mergers and acquisitions, and sensitive operational communications.

3.3.3 Security in Third Party Agreements

LegalMaps Legal Department is responsible for interpreting and answering questions concerning legally related issues, reviewing and preparing necessary contracts, and assisting with the interpretation of laws and regulations. All third party contracts and agreements must be initiated or reviewed by the LegalMaps Legal Department.

3.3.3.1 Soliciting or Obtaining of LegalMaps Information

No third party services pertaining to the electronic or physical handling of customer or LegalMaps information will be solicited or obtained without the written approval of the Director of Information Security or their delegate.

3.3.3.2 Handling of LegalMaps Information

No third party services pertaining to the electronic or physical handling of customer or LegalMaps information classified as Confidential or above may be activated without the written approval of the Director of Information Security or their delegate.

3.3.3.3 Third Party Service Provider Contracts

Third party service provider contracts must be obtained through approved LegalMaps Legal Resources. All contracts with third party service providers must be reviewed with the Legal department prior to execution. If customer data or LegalMaps information is shared with the third party, contract language that specifically addresses applicable laws and regulations must be included in the contract.

3.3.3.4 Third Party Source Code

Where third party software will be developed or used to perform critical business functions, the source code must be either licensed to and in the custody of LegalMaps, or the third party must periodically provide source code to a third party agent who will hold the source code in escrow. This policy does not apply to commercial off-the-shelf software.

3.3.4 Security Standard for Disclosure of Details Related to LegalMaps Security

This policy and LegalMaps' LegalMaps Security Standards establish the LegalMaps Security standard for the dissemination of security information and are considered Confidential and for internal distribution only unless classified otherwise by LegalMaps Security or Legal.

3.3.5 Security Standard for Distribution Lists

This policy and LegalMaps' LegalMaps Security Standards document established the LegalMaps Security standard for Distribution Lists.

3.3.6 Security Standard for Security Reviews

This policy and LegalMaps' LegalMaps Security Standards establish the LegalMaps Security standard for Security Reviews.

4 Asset Management

Asset management is an important aspect of security planning in a complete security program. By evaluating the type of information in question and its associated value, a level of classification can be assigned to the information that then will be used to simplify policy implementation and enforcement. The following chapter includes important policy matrices that may be used frequently to interpret required controls once a data classification level has been assigned to an Information System.

4.1 System Category and Minimum Controls

At a minimum, LegalMaps Information Systems are required to have the following:

- Assignment of operational responsibility and asset ownership;
- Security planning activities, including development of security rules, risk assessment, security training, and the implementation of other operational, management, and technical controls; and
- Periodic review of security controls to assure that management, operational, and technical controls are appropriate and functioning correctly.

Note: The Information System/asset owner is ultimately responsible for the classification of information.

4.1.1 Information System Minimum Controls

At a minimum, all LegalMaps Information Systems shall include the following:

- ***Assign Responsibility for Security***. Assign security responsibility for each Information System to an individual knowledgeable in the information technology used in the Information System and in providing security for such technology, including the management of security controls such as identification and authentication.
- ***Review of Security Controls***. An independent or self-review of the security controls in each Information System must be conducted when significant modifications are made to the Information System, or at least **annually** if no significant modifications occur. Reviews should assure that assignment of responsibility for security, management authorization to process for an Information System, and operational, personnel, and technical controls are functioning effectively.

The following should be completed prior to an Information System being migrated into production:

- Risk Assessment documentation;
- Vulnerability/Penetration scanning of the application from internal networks based on Information System classification;

Software, data, and other information classified as **CONFIDENTIAL** or above (see Section 4.3.3 *Information Classification Guidelines*), made available on LegalMaps Information Systems, should be protected by the following mechanisms:

- Information is obtained and maintained in compliance with any contractual, data protection legislation, and privacy requirements. See Section 12.1, *Compliance with Legal Requirements*;
- Information will be protected during the collection process and when stored by means of acceptable encryption or comparable security measures based on the classification of the information. See the Section 7.13 *Encryption Requirements*;
- Firewalls capable of stateful inspection must be implemented to restrict access to only allowed network protocols and secure connectivity to back-end systems by limiting access to only those host and protocols required for production communications and support;

- Intrusion Detection/Prevention Systems, both host and network-based, must be implemented for all Information Systems processing Confidential or Highly Restrictive information, where applicable.

4.2 Hardware/Software Management

The hardware/software management of assets is the responsibility of the asset owner and authorized departments within LegalMaps as noted in the following subsections.

4.2.1 Inventory of Assets

Documentation for each LegalMaps Information System must include an inventory of all assets. An inventory of assets should be included within the maintained system documentation.

4.2.2 Procurement of Assets

All hardware and software will be procured, installed, and managed through LegalMaps authorized channels.

4.2.3 Remote Access Products

Only remote access products that have been approved by LegalMaps Security may be implemented and used.

4.2.4 Asset Compliance with Laws and Agreements

All computer software, applications, and programs must be used in strict compliance with all applicable laws, software licensing agreements, copyright laws, and LegalMaps policies. This includes both vendor-provided software and LegalMaps-developed software.

4.2.5 Alteration of Assets

LegalMaps computer equipment must not be altered or added to in any way (e.g. upgraded processor, expanded memory, or extra circuit boards) except by approved LegalMaps personnel. All maintenance, upgrades, and repairs must be coordinated through LegalMaps authorized channels.

4.2.6 Use of External Hardware/Software Tools

Unless specifically authorized by LegalMaps Security, users must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise security. Examples of such unauthorized tools include those which defeat software copy-protection, discover confidential passwords, identify security vulnerabilities, discover system or network topologies, remove evidence if misuse, or intercept data in transit.

Tools that are used by LegalMaps network engineers shall be reviewed and approved based on the product, not for an individual or individual instance. This is to eliminate the need to approve every instance for network engineering to resolve problems.

4.2.7 Mobile Data Storage Devices

External mobile data storage devices are prohibited. The following storage devices will no longer be issued without approval from LegalMaps Security:

- PCMCIA Hard drive (Hard Drive PC Card)
- CD or DVD Burners
- External Hard Drives (USB & Firewire)
- Zip Drives
- CD or DVD Burning Software
- Flash Drives

- USB Keys
- Jump Drives

Personally-owned Peripheral/Mobile Storage devices are NOT allowed to attach/connect to LegalMaps assets except for the purpose of recharging a mobile device's battery.

4.2.8 Hand Held Devices

Hand held, Personal Digital Assistants ("PDAs") or similar devices are a rapidly evolving class of computer. The controls mentioned throughout this policy for computers also apply to hand held devices where possible.

4.2.8.1 Personal Hand Held Devices

Personal Digital Assistants ("PDAs") or similar devices must not be used for LegalMaps business purposes unless they have been configured with the necessary security controls by LegalMaps Security.

4.2.8.2 Hand Held Devices Containing Sensitive Information

Hand-held devices containing sensitive information must have the data protected while in storage and encrypted while in wireless transmission, in transmission outside of LegalMaps, or in other situations of transport where unauthorized individuals may have access.

4.2.8.3 Transfer of Data To/From Hand Held Devices Containing Sensitive Information

Sensitive information resident on hand held devices must not be copied, replicated, or synchronized with another computer or hand held device unless the other computer or device has security controls implemented by LegalMaps or a LegalMaps-approved contracted vendor.

4.2.9 Ownership of Assets

All information and resources must have an Information System Owner that is assigned security responsibility for the asset.

Each asset owner must adhere to the following requirements and responsibilities:

- Responsible for classifying assets and resources into one of the four defined sensitivity levels (see Section 4.3.3 *Information Classification Guidelines* for more details.)
- If the owner is unsure at what level the asset or resource should be classified, then the asset or resource must be assumed and classified to be the most sensitive level.
- If a system contains information from multiple sensitivity classes, then it must be classified at the highest level of information within the system.
- Responsible for determining who is allowed access to the asset or resource.

4.2.10 Acceptable Use of Assets

To provide for computer hardware, software, and other necessary business equipment being used in accordance with approved LegalMaps business practices, users must adhere to acceptable use of LegalMaps assets to reduce the risk of introduction of viruses, malicious code, or other threats.

LegalMaps assets, and assets managed on behalf of LegalMaps, must be only used for holding and running LegalMaps owned software and data. LegalMaps assets must NOT be used for running or storing applications or data which:

- Have not been purchased by or on behalf of LegalMaps
- Support any private or non-LegalMaps business ventures
- Allow access to the Internet outside the control of the LegalMaps proxy servers.

- Taking photos or establishing video conferencing sessions (via integrated or USB webcams) unless they are approved devices and use approved video conferencing software programs.

4.2.10.1 Use of Non-LegalMaps Systems: Information system users, including consultants and temporary workers, must not bring non-LegalMaps owned computers, computer peripherals, portable electronic devices, or computer software into LegalMaps facilities without prior authorization from LegalMaps Security.

Personally-owned devices such as smartphones and tablets/iPads may be used only to receive corporate email if approved by IT and assuming the required, corporate-approved security software is installed on the device. The employee's department or manager may be responsible for any costs associated with installing the corporate-approved security software onto the device. Upon installation of the corporate security and/or email software onto a personally-owned device LegalMaps reserves the right to monitor, confiscate, investigate, and/or revoke corporate email capabilities on those devices at any time.

4.2.10.2 Use of Shared/Floater Laptops: LegalMaps laptops are not to be shared or floated among LegalMaps users or groups. Laptops shall be individually assigned for use.

4.2.10.3 Phone/Fax: Phone and fax systems are intended to be used for LegalMaps business purposes. Phone and fax systems shall not be used for unlawful activities, including violation of copyright laws or violation license agreements. The following measures should be taken when using phone and faxes:

- Telephone authentication procedures should be followed at all times. It is imperative that callers are properly identified before sensitive information is discussed.
- Be aware of who is near when discussing sensitive information. Do not discuss sensitive information in elevators, cafeterias, or other public places.
- Cell phones that contain built-in cameras, whether owned by LegalMaps or the user, may be carried into approved LegalMaps facilities but must not be used to take photos while inside LegalMaps facilities or on LegalMaps premises. LegalMaps reserves the right to prohibit carrying of cell phones into LegalMaps facilities or areas as needed (such as facilities containing sensitive information.)
- When faxing sensitive information, always verify the recipient's fax number.
- When faxing, request the recipient or an authorized individual to pick up the faxed document without delay.
- Sensitive fax documents should not be left unattended on or by fax machines. Fax documents should be handled according to their data classification.
- Corporate fax servers should be used instead of manual faxes whenever possible.
- When multiple faxes are to be sent at one time, a file folder should be used to separate each fax document.
- Faxes should be securely configured.
- Fax machine owners must check the date/time on their machines at least twice annually to validate accurate times are being maintained.
- An approved LegalMaps cover page should be used on all faxes. This cover page shall contain no sensitive information and include the following notice:

  The information in this transmittal is personal and confidential. It is intended solely for the use of the individual or entity named above. Any reading, copying, disclosure, appropriation, or dissemination of the contents of this transmission by anyone other than the named recipient is strictly prohibited. If

you have received this communication in error, please call +1 612 886 8300 between the hours of 7am and 8pm, Monday to Friday. Thank you for your assistance.

4.2.10.4 Electronic Mail (E-Mail): E-mail systems are intended to be used for business purposes. E-mail systems may not be used for unlawful activities, including violation of copyright laws or violation of any license agreements.

4.2.11 Security of LegalMaps Hardware and Equipment

All computer hardware and other necessary business equipment must be properly secured at all times. Appropriate steps must be taken to secure equipment against theft or damage. The steps users should take include, but are not limited to:

- Securing laptops and other equipment to user's desk using a cable and padlock
- Enforcing the requirement that any equipment left in your vehicle is not visible. Equipment should be locked in the trunk of a user's vehicle. If a trunk is not available, LegalMaps equipment should be kept with the user at all times.

4.2.12 Implementation of Hardware/Software and Equipment

All computer hardware, software, and equipment must be implemented in accordance with LegalMaps installation/implementation standards.

4.2.12.1 All hardware and equipment must be installed and configured by the appropriate LegalMaps or authorized LegalMaps support person, not the end-user.

4.2.12.2 All default IDs (e.g. Guest) and passwords should be removed, changed or disabled on all devices.

4.2.12.3 Any non-required communication ports and/or services (e.g. pop mail, ftp, instant messaging) should be disabled prior to imaging/commissioning and allocating any equipment.

4.2.12.4 To enforce the requirement that areas such as home folders, network resources, and account IDs have been established in accordance with LegalMaps standards, users must not install or configure such equipment or software unless they have prior approval from their immediate management and a member of LegalMaps Security.

4.2.13 Decommissioning of Hardware and Equipment

Department managers are responsible for the prompt and proper disposal of surplus property no longer needed for business activities in accordance with procedures established by LegalMaps Security, including the irreversible removal of information and software.

4.2.13.1 All hardware and equipment must be decommissioned by an appropriate LegalMaps or LegalMaps approved contractor.

4.2.13.2 All software and data must be removed prior to the transfer or disposal of hardware or equipment.

4.2.13.3 A full format of the hard drive must take place prior to re-imaging or re-use. LegalMaps conforms to US Department of Defense clearing and sanitizing standard DoD 5220.22-M. US Department of Defense in the clearing and sanitizing standard DoD 5220.22-M recommends the approach "Overwrite all addressable locations with a character, its complement, then a random character and verify" for clearing and sanitizing information on a writable media. The LegalMaps standard policy is to do 7 passes

4.2.13.4 When a hard drive is to be decommissioned, the hard drive should be removed, degaussed and physically damaged in such a way to render the hard drive unusable.

4.2.13.5 When storage media such as tape is to be decommissioned, the media is to be degaussed and overwritten as outlined in Section 4.2.13.3 above.

4.2.14 Software Licensing

LegalMaps licenses the use of computer software from a variety of companies. LegalMaps does own this software or its related documentation and, unless authorized by the software developer, does not have the right to copy it. US and European copyright laws prohibit the illegal reproduction of software and may result in criminal penalties, fines, and imprisonment. LegalMaps users who make, acquire, or use UNAUTHORIZED copies of computer software or who install any unapproved software shall be disciplined appropriately up to or including termination.

4.2.14.1 Software on local area networks, LegalMaps workstations (including personal computers issued to LegalMaps employees or contractors) or on multiple machines, shall be used by LegalMaps users in accordance with the software licensing agreement.

4.2.14.2 LegalMaps workstations (PCs/Laptops) are LegalMaps assets and all software must obtain appropriate licensing.

4.2.14.3 If the software has not been issued by LegalMaps or an LegalMaps-approved/contracted vendor, it must be removed from the workstation.

4.2.14.4 Software licensing is governed by the Enterprise Software Management Policy.

4.3 Information Classification

Information classification assists in the process of resources receiving an appropriate level of protection. Information should be classified to indicate the need, priorities, and degree of protection. Information has varying degrees of sensitivity and criticality. Some items may require an additional level of protection or special handling.

The security classification given to the Information System shall become the minimum classification assigned to all the individual assets that make up the Information System. Some individual assets may be assigned a higher classification than the Information System, and must be noted as such, but an asset can never be of a lower classification than the overall Information System it is a part of.

LegalMaps procedures regarding data security and classification shall require that information be:

- Identified as to its classification (i.e. Public, Internal Use Only, Confidential or Highly Restricted);
- Accessed, used and disposed of in a manner commensurate with the information's classification and with LegalMaps disposition and retention polices/guidelines/schedules and procedures;
- Made secure against unauthorized creation, updating, processing, outputting, and distribution; and
- Appropriately secured and not accessible to non-approved users when not in use.

4.3.1 Identifying Sensitive Information

Sensitive information is any information in which the loss, misuse or unauthorized access to or modification of which could adversely affect the interests of LegalMaps, its clients, or the privacy of individuals.

4.3.2 Criteria for Determining Sensitivity

Determining sensitivity in an IT environment involves consideration of the system, data, applications, and type of user, which must be examined individually and in total. All systems and applications require some level of protection for confidentiality, integrity, and availability, which is determined by an evaluation of the sensitivity, and criticality of the information processed, the relationship of the system to the organization's mission, and the economic value of the system components.

Information and Information Systems are sensitive if one or more of the following criteria applies:

- ***Confidentiality*.** The information and/or Information System require protection from unauthorized disclosure and access. A requirement that private or confidential information not be disclosed to unauthorized individuals.
- ***Integrity*.** The information and/or Information System must be protected from unauthorized modification or destruction of information. The two facets of integrity are data integrity and system integrity. Data integrity is a requirement that information and programs are changed only in a specified and authorized manner. System integrity is a requirement that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
- ***Availability***. The information and/or Information System must be available on a timely basis to meet mission requirements or to avoid substantial losses. A requirement intended to assure that systems work promptly and services are not denied to authorized users.

Systems critical to the performance of LegalMaps' mission are sensitive. The data on each must be secured against unauthorized disclosure, modification, or loss, and against unacceptable system downtime. Nothing in this section shall be construed to prohibit the disclosure of information when such disclosure is required by law or is requested or authorized by the legal owner of the information.

4.3.3 Information Classification Guidelines

The following guidelines will assist in determining the classification of the information that an Information System stores, processes, or transmits. A combination of several requirements determines information's classification. Determination of confidentiality, integrity, availability, risks, and Information System role are required for proper classification and is the foundation of security planning within the organization.

4.3.3.1 Information Classification Levels

Classification	Description	Examples
HIGHLY RESTRICTED (Class 4)	Highly Restrictive is the most sensitive information classification and is intended for use strictly within LegalMaps. Unauthorized disclosure or manipulation could seriously impact LegalMaps. Only executives are authorized to designate LegalMaps information as Restricted.	Highly Restricted data may be merger and acquisition documents and corporate level strategic plans in development.
CONFIDENTIAL (Class 3)	Confidential is sensitive information intended for use within LegalMaps and authorized delivery to customers, business partners, and service providers. Unauthorized disclosure could adversely impact consumers, business customers, LegalMaps or our associates.	Private consumer data, DMS data, customers' member numbers and security digits, LegalMaps' associates login information, and pricing documentation.

INTERNAL USE ONLY (Class 2)	For internal use only is data that does not clearly fit into Restricted or Confidential classifications. Unauthorized disclosure would not likely adversely affect consumers, LegalMaps or its associates or customers.	The LegalMaps telephone directory and new employee training materials.
PUBLIC (Class 1)	The Public classification applies to information that has been approved by LegalMaps management for release to the public. There is no unauthorized disclosure of this information and it may be disseminated without potential harm.	Examples include product and service brochures, advertisements, and press releases.

4.4 Information Labeling and Handling

The Information classification guidelines should be used to categorize data into its appropriate data classification. If information control decisions need to be made, the business or operations manager should reasonably apply the most restrictive data classification possible based on the classifications defined in this policy.

- A secure environment is a physically secure area e.g. computer room, where written authorization is required in order to view or remove any information storage media (e.g. tape).
- If any member of staff finds a Confidential or higher item and it is not properly secured, it is their responsibility to secure it in accordance with the classification label attached to it.
- If a label is not found on a document, the document is to be considered Confidential.

Labeling and Handling Information Matrix

LABELING & HANDLING	PUBLIC (Class 1)	FOR INTERNAL USE ONLY (Class 2)	CONFIDENTIAL (Class 3)	HIGHLY RESTRICTIVE (Class 4)
Storage of Information (electronic)	No security control requirements	Site/Department storage should be adequate to prevent casual disclosure.	Information may require encryption. Where it does, approved methods must be used.	Sensitive fields must be encrypted using company-approved methods of encryption.
Storage of Information Media	No security control requirements	Site/Department storage should be adequate to prevent casual disclosure.	Backup media must be kept in locked storage or a secure environment and restricted to authorized persons.	
Labeling of Information (documents only)	Must be labeled with the classification	Must be labeled with the classification	The documents must be marked 'CONFIDENTIAL' and/or physically separated and protected during storage	The documents must be marked 'HIGHLY RESTRICTED' and/or physically separated and protected during storage. Copies must contain a unique ID.
Labeling of Media	Media must be externally labeled with the appropriate data classification at all times. Labeling must appear on all manifestations of the information with the exception of copyrighted software.			

Disposal of Information (electronic)	Removal of Directory entry for file.		
Disposal of Physical Media (e.g. paper / magnetic media)	No Restrictions	Media must be Regarded as CONFIDENTIAL and be disposed of securely using approved methods and based on retention strategies. Please refer to LegalMaps' LegalMaps Security Standards document, Section 22.	Information must be Disposed of securely using approved methods and based on retention strategies. A record must be kept of how, when and by whom the media was destroyed. Please refer to LegalMaps' LegalMaps Security Standards, Section 22.

4.4.1 Additional Requirements for Information Labeling and Handling

4.4.1.1 Electronic Storage of Sensitive information

Consumer data, public or private, must never be stored on a laptop or end user's PC. All other sensitive information may be stored on a laptop if it is encrypted using an approved LegalMaps methodology.

Only LegalMaps or service provider approved computers or digital media are allowed to handle LegalMaps information. Therefore, LegalMaps prohibits performing work with a user's personally owned computer, or burning or saving any LegalMaps data onto end user CDs, flash drives, or other portable digital media.

Customer data must never be stored outside of the country of origin without the express written approval of the Director of Information Security.

4.4.1.2 Removing Sensitive information from Facilities

Highly Restricted information, no matter the form, must not be removed from LegalMaps premises without the advanced approval of an LegalMaps executive and the Director of Information Security. Consumer information, no matter the form, must not be removed from LegalMaps premises without the advanced approval of the Director of Information Security. Delivery of consumer information to customers and LegalMaps approved service providers, such as for performing data backup storage, are exempt from this requirement.

4.4.1.3 Special Considerations for Handling Highly Restricted Data

Highly Restricted information in hardcopy (printed) form may be sent by trusted courier only. Regular or registered mail is prohibited. Highly Restricted information must not be discussed or displayed in public. Highly Restricted information must not be sent to an unattended fax machine unless the destination machine is in a locked room. If Highly Restricted information is released orally in a meeting, the speaker must communicate the sensitivity of the information beforehand.

4.4.1.4 Special Considerations for Handling Consumer Data

Users must never access their credit file or the credit file of anyone they know. Users shall never alter, change, update, or delete any authentic contents of a credit file unless properly authorized to do so. Users can only perform activities associated with their job function. Users shall immediately notify their manager when asked to improperly alter a credit file. Users shall immediately notify their manager if they believe or know any person is performing unauthorized disclosure, alteration, change, update, or deletion of a credit file.

4.4.1.5 Physical Handling Procedures

Sensitive LegalMaps information moved physically must be encrypted. If encryption is not available, the physical media must be shipped by a secure means using an approved courier.

4.4.1.6 Reporting a Security Incident

Please refer to Section 10.1 *Reporting Security Events* of this policy for further details regarding how to report a computer security incident.

4.5 Corporate Retention Requirements

Corporate Data Retention Guidelines for LegalMaps Security (in years unless otherwise specified)

Terms and Definitions:

- Official records are the archived versions of the native information.
- Online records are the original records in their native form, e.g. system/security logs within the system itself and physical forms with original signature rather than a copy.

Data Type	Official	Online	Domain	Description / Notes
Logical Security Device and Application Logs	**1 Years**	**90 Days (min.)**	Logical	Examples: Firewalls, Intrusion Detection/Prevention, Anti-Virus, Authentication Systems and Remote Access Systems
Operating System and Application Logs	**1 Years**	**90 Days**	Logical	Operating system and application specific logs concerning information relevant to security and system/application status.
Internet Based Systems	**1 Year**	**90 Days**	Logical	All access to files/databases containing sensitive information must be logged.
Payment Card Industry (PCI) Cardholder Specific Data (related to merchant transactions)	**1 Year + AR**	**90 Days + QR**	Logical	Refer to Payment Card Industry (PCI) Security Standards for more information.
Corporate E-mail Messages	**1 Year**	**1 Year**	Logical	Alternative means exist for longer retention upon user request and an approved Security Exception.
Router and Network Device Logs	**1 Years**	**90 Days**	Logical	Does not include network traffic; only configuration changes and information relevant to security such as authentication & access control.
Key Management Audit Trails	**LI**	**3 Years**	Logical	Audit trails shall be retained for a given key throughout the life and for three (3) years subsequent to the destruction and/or deletion.
Network Plans/Drawings/Diagrams	**LI**	**SU**	Logical	
Access Request Forms	**5 Years**	**N/A**	Logical	

Incident Reports – Logical (electronic)	**10 Years**	**1 Year**	Logical	Security incidents that may compromise the availability, integrity, and confidentiality of LegalMaps data and resources.
Incident Reports - Physical (hard-copy)	**10 Years**	**1 Year**	Physical	Physical Security specific incident reporting only.
User Physical Security Access Cards	**TE+AR**	**TE**	Physical	
User Physical Security Access Database	**1 Year**	**1 Year**	Physical	
Surveillance Video Tapes and Logs	**90 Days**	**90 Days**	Physical	
Visitor Sign-In Logs and Access Reports	**1 Year**	**1 Year**	Physical	
Investigation Reports – External	**10 Years**	**1 Year**	Physical	Physical Security specific investigations only.
Investigation Reports – Internal	**10 Years**	**1 Year**	Physical	Physical Security specific investigations only.
LegalMaps Security Investigations: Forensic and Incident Data and Reports	**LI**	**1 Year**	Investigations	All information related to the investigation of a security incident and forensic analysis.

Retention Policy Event Codes	**Additional Requirements:**
LI – Life (of corp., property, system, etc.)	Data stored for life (LI) must remain readable over the lifetime of the information. The media utilized to archive the information must be check at least every four (4) years for readability and applicability to modernized hardware and software requirements.
SU – Superseded	
TE – Termination	
QR – Quarterly Review	
AR – Annual Review	

5 Human Resource Security

Human Resources Security controls address security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to systems).

These controls are put into place to improve the security of a particular system (or group of systems). Human Resources security controls often require technical or specialized expertise and rely upon management activities and technical controls.

All other issues regarding users of the LegalMaps not covered herein are to be addressed by the Human Resources Department separately.

5.1 Prior to Employment

Potential LegalMaps users (applicant) cannot begin any position with or perform services for LegalMaps until a background investigation is completed. Human Resources should be consulted for the latest requirements regarding LegalMaps users outside of the U.S.

The background investigation should include the following controls (where allowed by law):

- Availability of satisfactory employment references.
- Drug Screening: Defined as a screening that tests for amphetamines, marijuana, opiates, methamphetamines, cocaine or the presence of dilution in the urine. The requirement of drug screen will be modified to comply with state law if the individual will be employed in a state that does not permit the above.
- A check (for completeness and accuracy) of the applicant's application.
- A check of the Office of Foreign Assets Control (OFAC) list.

- Verify the individual's identity through the I-9 process if applicable.
- A search for any type of criminal conviction and arrest (where allowed by law) will be conducted for all local and/or state jurisdiction where a potential user lived, worked and went to school for, at a minimum, the past seven (7) years. Individuals shall not have been convicted of any offenses related to fraud or financial crimes.

Where a job, either on initial appointment or on promotion, involves the person having access to information processing facilities, and in particular if these are handling sensitive information, e.g. financial information or confidential information, the organization will carry out a credit check. For staff holding positions of considerable authority this check should be repeated periodically or at least every 7 years.

This information should be handled in accordance with any appropriate legislation existing in the relevant jurisdiction.

5.1.1 Confidentiality Agreements

Users must sign a Confidentiality Agreement before being allowed to access LegalMaps Information Systems. The confidentiality or non-disclosure agreements are issued by the Human Resources department, and must be completed before access is granted. Thus, any IT Administrator (or anyone that grants user access) must check with Human Resources to confirm a Confidentiality or Non-Disclosure agreement is on file for the user.

When a user leaves LegalMaps, all information stored by that user on LegalMaps-owned or leased personal computers, electronic networks and other information-processing and storage devices remain the property of LegalMaps.

LegalMaps reserves the right to monitor and review the content of any electronic message or document for any business or legal purpose without informing the sender or recipient of that electronic message or the person in whose possession those computer files reside.

Violations of this LegalMaps Security Policy may expose a user to disciplinary action, including loss of employment.

5.1.2 Intellectual Property Rights

LegalMaps maintains ownership of all intellectual property created or maintained by LegalMaps resources or intrinsic knowledge. Duplication of any intellectual property for personal gain is strictly prohibited. Intellectual property will include, but not limited to, any of the items referenced below created or maintained in either hand written or electronic format.

- Data, Programs, or Applications
- Trade Secrets
- Network Configuration and Design
- Financial, Revenue, or Sales Figures
- Training Course Information
- Purchase Equipment Plans
- Manuals
- Customer Lists
- Source Code
- Business Plans
- Implementation Schedules
- Policies and Procedures

All intellectual property will be returned to LegalMaps upon demand.

5.1.3 Roles and Responsibilities

Users should be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment. Such awareness shall be provided by Security Awareness training, required periodically and for all new users.

5.1.4 Terms and Conditions of Employment

LegalMaps is a custodian of data and it is imperative that we hold the data securely and confidentially. Security events are treated seriously and will always result in whatever action is necessary to demonstrate that we take our custodianship seriously. Any unauthorized or illegal use of LegalMaps and/or customer data or systems is classified as a security event. Examples of security events include:

- Unauthorized access to LegalMaps consumer, commercial, asset or personal data.
- Unauthorized amendment of consumer, commercial, asset or personal data.
- Unauthorized disclosure of consumer, commercial, asset or personal data held within any LegalMaps Information System.

Security events could result in:

- User(s) being subjected to disciplinary action including dismissal without notice.
- LegalMaps and/or its users facing criminal prosecution.
- LegalMaps and its users being subjected to investigation by regulatory authorities.

5.1.5 During Employment

To support the efforts of both LegalMaps and its users to fulfill our legal obligations regarding consumer, commercial, asset and personal data, one must adhere to the following rules:

- **Never** access any consumer, commercial, asset or personal information unless it is for an appropriate business reason.
- **Never** change, update, or delete the details of any LegalMaps database unless you have the proper authority to do so.
- If you have been approached by anyone or if you know of any LegalMaps user violating these rules, you are required to immediately report it to LegalMaps Security.

5.1.6 Management Responsibility

It is management's responsibility to make sure their users adhere to this policy and report or take action on security events or out-of-compliance issues.

5.2 Security Awareness and Training

All users with access to any of LegalMaps Information Systems or Information must complete Security Awareness Training.

5.2.1 Security Awareness Program

LegalMaps Security will monitor and report on the participation and the effectiveness of the Security Awareness program.

5.2.2 Security Awareness Purpose and Goals

The purpose of Security Awareness, training, and education is to implement security requirements by:

- Providing awareness of the need to protect system resources;
- Educating and training users on the security skills and knowledge needed so system users can perform their jobs securely and consistently with LegalMaps security policies and procedures; and
- Building in-depth knowledge to design, implement, or operate security programs for organizations and systems as appropriate to job function and activities.

The Security Training and Awareness Program is intended to meet the following goals:

- All LegalMaps users involved with the management, operation, programming, maintenance, or use of LegalMaps Information Systems will receive training in computer security that is appropriate for their job responsibilities; and
- All new users will receive security orientation upon initial employment. The orientation can be given separately or as part of the existing new user orientation.

5.2.3 Security Awareness Program Responsibilities

LegalMaps Security is responsible for:

- Providing assistance such that security training goals are met; and
- Providing direction and priority to the Security Awareness training program.

Business Units: Individual Business Units are responsible for confirming that their users are:

- Trained on how to fulfill their security responsibilities prior to allowing them system access;
- Appropriately trained to what they need to know to use the system securely;
- Versed in the rules of the system before allowing them usage; and
- Periodically trained to assure that they continue to understand and abide by the applicable rules.

5.3 Internet/Intranet Usage Policy

Internet and Intranet usage must be in accordance with the Compliance Program and must comply with all applicable portions of this policy. LegalMaps provides the Internet to assist users in the performance of one's job. The Internet should be used for official LegalMaps business. However, incidental and occasional personal use of LegalMaps' Internet connection that does not interfere with LegalMaps' business is permitted. All LegalMaps systems accessing the Internet must be connected to the LegalMaps network. For example, LegalMaps laptops must connect to the LegalMaps network, either by being on premise at an LegalMaps office location or via VPN, before they are allowed to browse the Internet.

The Internet may not be used in any way that may be seen as insulting, disruptive, offensive, or harmful to morale. Examples of forbidden usage includes: adult oriented, hate, or sexually explicit websites.

5.3.1 Internet Connections

Accessing the Internet, for conducting LegalMaps business, through connections other than LegalMaps authorized methods is prohibited.

5.3.2 Posting to Social Media

Posting to Social Media Groups (Facebook, Twitter, Snapchat, etc.), internet forums, or other public Information Systems of any message(s) directly or indirectly referencing LegalMaps or identifying the participant as a

LegalMaps representative is prohibited without an approved Security Policy Exception. Please refer to LegalMaps' other corporate policies regarding social networking communications for additional details.

5.3.3 Establishing or Modifying Web Sites

Users are prohibited from establishing or modifying web sites, web pages, or bulletin boards in connection with LegalMaps except through approved LegalMaps methods and authorized channels.

5.3.4 Web Sites Created with LegalMaps Resources

Users must not create, maintain, or administer personal web sites, web pages, or bulletin boards through the use of LegalMaps systems or resources.

5.3.5 Internet Accessible Connections and Devices

All LegalMaps network connections or network attached devices directly accessible from the Internet (or any other publicly-accessible computer network) including, but not limited to, Internet commerce servers, database servers, and web servers must be protected by approved security mechanisms, configurations, and security architecture.

5.4 Email Usage

Email usage must comply with all applicable portions of this policy. LegalMaps provides email to assist users in the performance of their job. Email should be used for official LegalMaps business. However, incidental and occasional personal use of email that does not interfere with LegalMaps' business is permitted.

Email may not be used in any way that may be seen as insulting, disruptive, offensive, or harmful to moral. Examples of forbidden transmissions include: sexually explicit messages, cartoons, or jokes; unwelcome propositions or love letters; ethnic or racial slurs; chain letters; or any other message that can be construed to be harassment or disparagement of others.

5.4.1 Forward of Email

Users must not configure their LegalMaps provided email system to automatically forward messages or attachments to non-LegalMaps email systems.

5.4.2 Replication of Email

Replication (copying) of LegalMaps email to or from any hand held computer or other personal computing device such as laptop or desktop computer is prohibited unless both the sending and receiving device have security controls implemented by LegalMaps. For example, synchronizing a PDA containing LegalMaps email with a non-LegalMaps computer is prohibited. Thin-client or browser-based technologies may be approved by LegalMaps Security (i.e. Outlook Web Access) before implementation.

5.5 Terms and Conditions of Employment

LegalMaps users must adhere to all policies and procedures for proper use of LegalMaps information systems.

5.5.1 Disciplinary Process

Violation of these policy requirements is subject to disciplinary action. The appropriate action is determined by a user's manager in coordination with the LegalMaps Human Resources Department.

5.5.2 Termination or Change of Employment

Supervisors must immediately notify their Security Administrator(s) or Human Resources representative when a user's relationship with LegalMaps is terminated or a temporary, consultant, or other third-party contract has ended in order for system access to be removed.

5.5.3 Termination or Transfer Responsibility

When a user is terminated from LegalMaps or transfers to another position, the supervisor must make arrangements to shift responsibility for the user's data to another user and/or archive or destroy the data as appropriate within thirty (30) days of the termination or transfer. For example, this would include computer data files such as email, word documents, spreadsheets, and hard copy files.

5.5.4 Return of Assets

Upon termination of a user's relationship with LegalMaps, the supervisor must make arrangements to promptly collect LegalMaps assets, access control devices, laptops, pagers, PDAs, tokens, badges, keys, cell phones, operating manuals, department procedures, and other LegalMaps sensitive information from the user. Supervisors must confirm that these assets are properly controlled and forwarded to the appropriate areas for redeployment or disposal as appropriate.

5.5.5 Removal of Access Rights

Upon termination of a user, all system IDs belonging to users who leave LegalMaps should be deleted immediately after the user has completed their last working day. Managers are responsible for notifying Human Resources or Security Administration of dismissals so that their IDs can be removed.

6 Physical and Environmental Security

To provide for information, data, and equipment being adequately protected against unauthorized access and/or use, LegalMaps has outlined the following physical and environmental security elements to aid in the availability, integrity, and confidentiality of information and systems.

Physical security involves the use of locks, access/photo ID badges, alarms, procedures, and similar measures (alone or in combination) to control access to the Information System. Physical and environmental security controls are implemented to protect the facility housing the system resources, the system resources themselves, and the facilities used to support their operation from theft, espionage, terrorism, waste, fraud, abuse, or damage by accident, fire, and environmental hazards.

LegalMaps shall adequately protect its facilities used to process, transmit, or store sensitive LegalMaps information in support of critical operations and missions. The specific security policies for each LegalMaps physical location may vary and will be based upon the individual risk assessment document prepared for that facility. If a risk assessment by LegalMaps Security determines that a facility does not have sufficient physical security controls in place to safeguard LegalMaps equipment or data then compensating controls, such as encryption of desktop hard drives, may be required.

6.1 Secure Areas

Adequate security measures must be in place to protect computer, communications equipment, and data.

Physical access controls must restrict the entry and exit of personnel (and often equipment and media) from an area, such as a service center, computing center, data center, or room containing critical devices.

LegalMaps reserves the right to conduct random searches of bags (purses, book bags, shopping bags/boxes, etc.) and briefcases on LegalMaps premises.

6.1.1 Physical Security Perimeter

The following physical perimeter controls shall be implemented where appropriate:

- The security perimeter should be clearly defined.
- The perimeter of a building or site containing information processing facilities, or any other LegalMaps owned property, shall be physically sound (i.e. there should be no gaps in the perimeter or areas where a break-in could easily occur). The external walls of the site shall be of solid construction and all external doors should be suitably protected against unauthorized access, e.g. control mechanisms, bars, alarms, locks etc.
- Where appropriate, CCTV should be used to monitor and record access to LegalMaps sites to deter intruders, protect users and be used as a basis for evidence in any civil or criminal proceedings or internal investigation.
- All fire doors on a security perimeter shall be alarmed and should have automatic closing devices on all doors and be secured at all times in accordance with approved fire procedures for that location.

6.1.2 Physical Entry Controls

The following physical entry controls shall be implemented where required by policy or deemed appropriate by LegalMaps Security:

- Only authorized and authenticated users are permitted access to secure areas.

- A staffed reception area or other means to control physical access to the site or building must be in place. Access to sites and buildings should be restricted to authorized personnel only.
- Upon employment with LegalMaps, all users receive an access/photo identification badge (ID). This ID badge allows access to those areas required by the user. Management is responsible for notifying Physical Security regarding the type of access each user requires.
- Entry systems such as swipe, proximity cards, or smart cards should be utilized and grant access to buildings on a job needs basis.
- All users should sign in/out when an electronic form of grant access is not available.
- All users must wear their access cards bearing their name and/or photo, in a clearly visible manner, at all times when entering and working at any LegalMaps business location.
- Any authorized badge holder who does not have their ID badge must enter through the Main facility entrance and report to their management or appropriate security personnel for temporary access. Temporary badges are issued for no more than one day.
- Facilities shall not post any external indication of sensitive operations taking place within the facility (i.e., signs should not indicate sensitive operations within, no directories or floor-plans that indicate the location of sensitive areas should be available to the public).
- Personnel leaving the building with proprietary or confidential information and/or equipment must have the appropriate authorizations (contact LegalMaps Security for details).

6.1.2.2 Visitor Controls

- All visitors must be appropriately signed in at the reception desk, or appropriate authority, at each LegalMaps site. Visitors must not be allowed to access any LegalMaps site without being under the supervision of a LegalMaps user.
- All visitor badges must be returned to the reception desk or appropriate authority when a visitor leaves any LegalMaps site. It is the responsibility of the LegalMaps sponsor who is accompanying the visitor to confirm the visitor is properly signed out and that any temporary passes or other items loaned for the duration of the visit are returned to LegalMaps.

6.1.2.2.1 Visitor Access Requirements

- Tours are defined as a visitor, or collection of visitors, that visit a LegalMaps Data Center facility for informational purposes only with no intent of performing work related duties for LegalMaps or its subsidiaries. Data Center Tours are prohibited under any circumstances without an approved Security Policy Exception.
- All visitors entering LegalMaps facilities during normal working hours must sign the visitor's log. When security officers are present all visitors will receive a temporary visitor badge upon exchange of a form of valid government issued identification. The visitor badge must be worn at all times while in the building. An authorized badge holder is responsible for escorting the visitor and confirming that all LegalMaps procedures are followed. Before access is granted to a LegalMaps Data Center, special access rights may be required. All access to the Data Center must be authorized and logged.
- Visitors are not permitted to carry briefcases, boxes or other containers into any secure data processing areas without approval from Global/Physical Security. Any such items removed from the facility are subject to search.
- When leaving the facility, the badge holder will escort the visitor to the main lobby and confirm that the temporary badge is returned.

- During non-standard business hours (any day 6:00pm through 7:00am, and all holidays) only authorized badge holders may enter the facility. Family members of authorized badge holders may be allowed under standard visitor access requirements. The badge holder assumes full responsibility for confirming all processes and procedures are followed.
- No cameras or recording devices are allowed inside secure data processing areas without an approved Security Policy Exception.

6.1.2.2.2 Visitor Registration Program

The following standards are provided to facilitate the implementation of a visitor registration program:

- A visitor registration program should be implemented and maintained at each LegalMaps facility. All LegalMaps visitors should be required to sign in and sign out upon each arrival and departure.
- The visitor registration sheet should contain the following information at a minimum:
  - Date
  - Arrival and Departure times
  - Visitor's name and visitor's company
  - Name of user sponsor and signature
  - Visitor badge serial number
  - Signature of the visitor
- All contract services providers who do not pass the approved background check program shall be required to adhere to visitor documentation processes.
- The provision of a continuous escort to all non-user visitors is required.
- Visitor logs must be retained for a set period of time. Refer to the Section 4.5 *Corporate Retention Requirements* of this document for more details.

6.1.2.3 Additional Requirements for Data Center Access

Routine entry to LegalMaps Data Centers should be allowed only to individuals whose primary workstation is within the workplace area or required by their job responsibilities. Entry by persons whose primary workstation is not within the area, or as required by their job responsibility should be logged and authorized on an as-needed basis. Authorized support personnel should be kept under visual control.

6.1.3 Securing Offices, Rooms, and Facilities

A secure area may be a locked office or several rooms inside a physical security perimeter, which may be locked and may contain lockable cabinets or safes. The selection and design of a secure area should take account of the possibility of damage from fire, flood, explosion, terrorism, civil unrest, and other forms of natural or man-made disaster. Account should also be taken of relevant health and safety regulations and standards. Consideration should be given also to any security threats presented by neighboring premises, e.g. leakage of water from other areas.

A secure facility shall be unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building identifying the presence of information processing activities.

The following are "secure area" requirements:

6.1.3.1 Physical access to data and operation centers, telecommunications switch rooms, technology inventory rooms, network closets, and other appropriate locations where technology infrastructure components reside

must be restricted to only those whose job responsibilities require their access to these locations. Access must be recorded.

6.1.3.2 Support functions and equipment, e.g. photocopiers, fax machines, should be located appropriately within the secure area to avoid demands for access, which could compromise information.

6.1.3.3 Doors and windows must be locked when unattended and external protection should be considered for windows, particularly at ground level.

6.1.3.4 Suitable intruder detection systems installed to professional standards and regularly tested must be in place to cover all external doors and windows. Unoccupied areas should be alarmed at all times. Cover should also be provided for other areas, e.g. computer room or communications rooms.

6.1.3.5 Information processing facilities managed by LegalMaps must be physically separated from those managed by third parties.

6.1.3.6 Directories and internal telephone books identifying locations of sensitive information processing facilities must not be accessible by the public.

6.1.3.7 Hazardous or combustible materials must be stored securely at a safe distance from a secure area. Bulk supplies such as stationery must not be stored within a secure area until required.

6.1.3.8 Fallback equipment and back-up media shall be sited at a safe distance to avoid damage from a disaster at the main site.

6.1.3.9 Computers operating as servers must be located in a data center or other secured location approved by LegalMaps Security.

6.1.4 Protecting Against External & Environmental Threats

Due care should be taken to minimize threats from external and environmental threats.

6.1.4.1 Physical barriers should, if necessary, be extended from real (true) floor to real (true) ceiling to prevent unauthorized entry and environmental contamination such as that caused by fire and flooding.

6.1.4.2 Users should take reasonable precautions to prevent damage to computer equipment due to exposure to the environment (i.e., water, food, drinks, etc.). If equipment is damaged, users must promptly contact the LegalMaps Help Desk.

6.1.4.3 Smoke alarms and automatic extinguishing systems shall be in place and in working order.

6.1.4.4 Air control conditioning systems should be operational and handle sufficient volume to compensate for the operating conditions at each site.

6.1.4.5 LegalMaps business sites must have maintenance agreements in place for such equipment and be assigned to an appropriate owner.

6.1.5 Working in Secure Areas

All sensitive LegalMaps data, including customer data, whether in hard copy or on electronic devices such as laptops, PDAs, hard disk drives, diskettes, magnetic tapes, and CDs must be physically secured when not in use.

6.1.6 Alternative Work Site

The security of LegalMaps property at an alternative work-site is just as important as it is at LegalMaps office(s). At alternate work-sites (i.e., hotel room, home, another company), reasonable precautions and due care must be taken to protect LegalMaps' hardware, software, and information from theft, damage, and misuse. Please reference this policy and the LegalMaps Security Standards document, as well as contact LegalMaps Security and/or Human Resources, to determine the appropriate security controls needed for an alternative work-site.

6.1.7 Delivery and Loading Areas

Delivery and loading areas should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. Security requirements for such areas should be determined by a risk assessment of the environment in question. The following controls are required:

6.1.7.1 Access to a holding area from outside of the building must be restricted to identified and authorized personnel.

6.1.7.2 The holding area should be designed so that supplies can be unloaded without delivery staff gaining access to other parts of the building.

6.1.7.3 The external door(s) of a holding area must be secured until arriving cargo has been validated and when the internal door is opened.

6.1.7.4 Incoming material shall be inspected for potential hazards before it is moved from the holding area to the point of use.

6.1.8 LegalMaps Equipment

The following standards are provided for the accountability and retention of LegalMaps equipment:

6.1.8.1 LegalMaps equipment and tools should be permanently marked for identification purposes. Any theft of LegalMaps property or tools shall be reported in accordance with Section 10.1, *Reporting Security Events*.

6.2 Equipment Security

LegalMaps equipment should be physically protected from security threats and environmental hazards.

Protection of equipment, whether at an LegalMaps facility or used off-site, is necessary to reduce the risk of unauthorized access to data and to protect against loss or damage. The following controls should be adhered to, at a minimum:

6.2.1 Physical Security of Equipment and Data

All sensitive LegalMaps data, including customer data, whether in hard copy or on electronic devices such as laptops, PDAs, hard disk drives, diskettes, magnetic tapes, and CDs must be physically secured when not in use and/or not in person. Physical security includes access-controlled measures such as locking materials in secured cabinets, etc.

6.2.2 Physical Security of Servers

Servers, including but not limited to mainframes and midranges, must be stored and managed in a trusted/secure environment that limits physical access to the devices so that only authorized and authenticated parties are provided access.

6.2.3 Network Device Equipment

Physical access to network device equipment (access points, routers, switches, hubs) must be properly restricted so that only appropriate personnel have access to them.

6.2.4 Wiring Cabinets/Closets

All wiring cabinets/closets must be physically secured so that only appropriate personnel have access. Network cables, except workstation cabling (where some exposure is required), shall not be exposed and should be inspected routinely.

6.2.5 Diagnostic Equipment

Authorized administrators will control distribution and use of diagnostic monitoring equipment (software and hardware), such as protocol analyzers and packet sniffers, that are limited to authorized personnel.

6.2.6 Environmental and Natural Hazards

Information Systems shall be reasonably protected against all anticipated environmental and natural hazards to reduce the risk as much as possible.

6.2.6.1 Environmental events must be monitored in a manner that alerts personnel to impending threats.

6.2.7 No Food, Drink, or Smoking in Data Centers

There must be no eating, drinking and smoking within data centers or computer rooms/closets other than designated areas.

6.2.8 Non-LegalMaps Equipment

Computer/communications hardware not in compliance with LegalMaps' technical architecture or not owned or leased by LegalMaps is not permitted to be used on LegalMaps property without proper approval. Privately owned hardware includes, but is not limited to; modems, peripherals, memory chips, additional hard drive, backup devices, scanners, printers, monitors, external/internal CD ROMS, sound cards, plug and play devices, PCs, laptops, servers, switches, routers, hubs, and firewalls.

6.2.9 Equipment Hosted at a Third Party

Any LegalMaps system that is hosted at a third party location (shared hosting environment) must be inaccessible to non-authorized and non-authenticated parties. Media handling, logging, and authorization must be consistent with this LegalMaps Security Policy.

6.2.10 Power Supplies

The following controls apply to information processing systems and equipment utilized for the support of critical business operations:

6.2.10.1 Information processing systems must be protected from power failures and other electrical anomalies, user workstations are an exception.

6.2.10.2 An Uninterruptible Power Supply (UPS) to support orderly close down or continuous running is required for equipment supporting critical business operations.

6.2.10.3 Contingency plans must include actions to be taken in the event of failure of the UPS.

6.2.10.4 UPS equipment must be regularly checked to provide adequate capacity and must be tested in accordance with the manufacturer's recommendations.

6.2.10.5 A back-up generator should be considered if processing is required to continue in the case of a prolonged power failure. If installed, generators shall be regularly tested in accordance with the manufacturer's instructions. An adequate supply of fuel should be available so that the generator can perform for a prolonged period as determined by a risk assessment.

6.2.10.6 If a back-up generator is used, the generator should be enclosed within a fence or in a location that prohibits unauthorized access.

6.2.10.7 Emergency power switches should be located near emergency exits in equipment rooms to facilitate rapid power down in case of an emergency. Emergency lighting must be provided in case of main power failure. Lightning protection should be applied to all buildings and lightning protection filters should be fitted to all external communications lines.

6.2.11 Cabling Security

Power and telecommunications cabling carrying data or supporting information services must be protected from interception or damage. The following controls must be deployed:

6.2.11.1 Power and telecommunications lines into information processing facilities should be underground, where possible, or subject to adequate alternative protection.

6.2.11.2 Network cabling should be protected from unauthorized interception or damage, for example by avoiding routes through public areas when and where possible.

6.2.11.3 Power cables should be segregated from communications cables to prevent interference.

6.2.11.4 For sensitive or critical systems further controls must include:

6.2.11.4.1 Installation of locked rooms or boxes at inspection and termination points;

6.2.11.4.2 Use of alternative routings or transmission media;

6.2.11.4.3 Use of fiber optic cabling;

6.2.11.4.4 Initiation of sweeps for unauthorized devices being attached to the cables.

6.2.12 Equipment Maintenance

Equipment should be correctly maintained to provide for its continued availability and integrity. The following controls are required:

6.2.12.1 Equipment should be maintained in accordance with the supplier's recommended service intervals and specifications.

6.2.12.2 Only authorized maintenance personnel can carry out repairs and service equipment.

6.2.12.3 Records must be kept of all suspected or actual faults and all preventive and corrective maintenance.

6.2.12.4 Appropriate controls should be taken when sending equipment off premises for maintenance (see also Section 7.8 *Media Handling* of this document, *Media Handling*, regarding deleted, erased and overwritten data). All requirements imposed by insurance policies should be followed.

6.2.13 Security of Equipment Off-Premises

Regardless of ownership, authorization must be obtained from LegalMaps Security for the use of any LegalMaps-owned Resource outside an organization's premises for information processing. The security provided shall be equivalent to that for on-site equipment used for the same purpose, taking into account the risks of working outside the organization's premises. The following guidelines should be considered:

a. Equipment and media taken off the premises should not be left unattended in any location other than its intended destination.
b. While equipment is in a user's possession, they will be held responsible for its safety and security.

6.2.13.1 Removal of Property

a. Where necessary and appropriate, equipment should be logged out and logged back in when returned. Spot checks should be undertaken to detect unauthorized removal of property.
b. Removal of property from an LegalMaps facility should be approved in advance.
c. Corporate assignment of a mobile computing or personal electronic device assumes, as part of the authorization process, that approval for removal of such property has been granted and authorized.

6.2.14 Secure Disposal or Reuse of Equipment

Information can be compromised through careless disposal or reuse of equipment. Storage devices containing sensitive information must be physically destroyed or securely overwritten rather than using the standard delete function.

All items of equipment containing storage media, including but not limited to hard drives, diskettes, tapes, USB drives, and tapes, shall be checked by LegalMaps IT personnel or authorized disposal vendors to confirm that any sensitive information and licensed software have been removed or overwritten prior to disposal. Damaged storage devices containing sensitive information may require a risk assessment to determine if the items should be destroyed, repaired or discarded.

Please refer to LegalMaps' LegalMaps Security Standards document, Section 22 for more details regarding standards for media sanitizing and disposal.

6.3 Office Moves

If and when it becomes necessary for relocation of a LegalMaps office and/or offices (due to renovation, change in space usage, emergency situation, lease expiration, etc.), LegalMaps equipment and documentation should be physically protected from security threats and environmental hazards.

Protection of equipment documentation (user manuals, configuration documents, etc.) is necessary to reduce the risk of unauthorized access to data and to protect against loss or damage. The following controls should be adhered to, at a minimum:

6.3.1 Physical Security of Equipment

All sensitive LegalMaps data, including customer and consumer data, whether in hard copy or on electronic devices such as servers, mainframes, PCs, laptops, PDAs, hard disk drives, diskettes, magnetic tapes, and CDs must be physically secured when not in use and/or not on person and cannot be encrypted to LegalMaps' encryption standard.

All information classified as Confidential or above should be boxed and sealed before transport as third parties potentially may be brought in for assistance with the moving of equipment.

6.3.2 Filing Cabinets and Drawers

All filing cabinets and drawers are to be emptied and documents reviewed for retention before the day of the move. Documents that are retained should be boxed and marked. Documents that are determined to be no longer needed per the Corporate Retention policy are to be shredded or disposed of in a secure shred container for shredding at a later time.

6.3.3 Wiping/Degaussing of Drives

All media that is to be disposed of in accordance with this Policy will be first sanitized utilizing current industry best practices. This process may include utilizing software products that permanently erase data by utilizing advanced algorithms to overwrite the data in randomized patterns. Other methods for sanitizing include hardware products such as degaussing devices that eliminate the recorded data on certain media by passing it through a strong magnetic field. Destruction of media may include shredding or other physical means of destruction. If necessary, a specialized vendor may be contracted to facilitate the shredding and disposal of physical media.

6.3.4 Movement of Equipment

Office moves will involve the transportation of valuable equipment such as PCs, servers, communications equipment, printers, copiers, and other machinery. This equipment is to be securely moved from office to office to protect LegalMaps from the loss and/or theft of equipment.

The Director of Information Security and Asset Protection is responsible for validating the security of all facilities containing operational corporate systems, that is, all corporate equipment that processes, transports, or stores information. Additionally, the Director of Information Security must approve all facilities containing operational corporate systems and must maintain an up-to-date inventory of all approved facilities. Only approved facilities can be used to house operational corporate systems.

7 Communications and Operations Management

7.1 Operational Procedures and Responsibilities

Responsibilities and procedures for the management and operation of all information processing facilities shall be established in accordance with this policy, e.g. procedures may be developed for business units or specific services that go to a greater detail level than within this policy but must remain in compliance with LegalMaps' security standards and IT control baselines. This includes the development of appropriate operating procedures and incident response procedures. Questions regarding LegalMaps security standards should be referred to the LegalMaps Security Compliance Team.

7.1.1 Documented Operating Procedures

The operating procedures as required by this policy should be documented and maintained. Operating procedures should be treated as formal documents and changes authorized by business unit management.

The procedures should specify the instructions for the detailed execution of each job (automated process or batch process) or administrative task of production Information Systems including, but not limited to:

a. Processing and handling of information;
b. Scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times;
c. Instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities;
d. Support contacts in the event of unexpected operational or technical difficulties;
e. Special output handling instructions, such as the use of special stationery or the management of confidential output, including procedures for secure disposal of output from failed jobs;
f. System restart and recovery procedures for use in the event of system failure.

Documented procedures should also be prepared for system maintenance activities associated with information processing and communication facilities, such as computer startup and close-down procedures, back-up, equipment maintenance, computer room and mail handling management and safety.

7.1.2 Change Management

All technology infrastructure (including, but not limited to firewalls, switches, routers, and other network devices) and application systems used for production processing at LegalMaps must employ a formal change control process. The change control process requires documentation of activities to be performed, potential impacts, applicable procedures, and peer review including authorized signature approval of reviewers. Emergency changes to the LegalMaps production environment must follow emergency change control procedures. This includes changes made to the LegalMaps production environment by third parties.

7.1.2.1 Change Management Controls for Production Implementation

The following controls must be in place before a system or application is placed or moved into production:

- Systems must be compliant with LegalMaps architecture, policies, and applicable security standards, or have an approved exception.
- Security services must be enabled.
- Security Administrator roles and responsibilities must be assigned.
- Security procedures must be documented and made available to the appropriate staff.
- System documentation must exist that describes all vital system components and processes necessary to support critical business operations.

7.1.3 Segregation of Duties

The purpose of separating duties is to reduce the risk (intentional or otherwise) of system misuse and interruption. It is recognized that staff limitations may necessitate the multitasking of personnel performing Security duties. However, when there is a perception of partiality, personnel are instructed to make the best decision based on the position they are currently filling.

LegalMaps shall implement separation of duties to the extent possible within the constraints of staff limitations. Situations that would give a single person the ability to approve their own critical work should be identified

and either eliminated or the supervisor/manager is responsible for maintaining a process for supervision and audit trails of any work done in that situation.

7.1.4 Separation of Environments

Testing, development, and production environments must be separate, either physically or logically from each other. Additionally, production and corporate networks must logically be separated.

Separating development, test, corporate, and production facilities is important to achieve segregation of the roles involved. Rules for the transfer of software from development to operational status must be defined and documented.

The following list of preventative measures shall be observed and adhered to in all environments (Development, Testing, Corporate, and Operations):

7.1.4.1 Users should not have access to compilers, editors, and other system utilities used to modify production applications or systems.

7.1.4.2 Test and development users should not have access to production applications or systems.

7.1.4.3 Development staff should only access production systems where controls are in place to monitor and supervise the activities with full audit trails. Such controls should include an end-point where the access is revoked after the activities have ended.

7.1.4.4 Development staff requiring access to production systems requires an approved Security Exception.

7.2 Third Party Service Delivery Management

A third party as applicable to this policy, is defined as a separate business entity or individual with no legal association to LegalMaps other than that of a contractual arrangement for services, is not an employee, authorized contractor, or subsidiary company. Examples would include clients of LegalMaps and business partners in which physical network connectivity exists for the purpose of information exchange.

Where there is a business need for such third party access, a risk assessment by LegalMaps LegalMaps Security should be carried out to determine security implications and control requirements. Compliance with the LegalMaps Security Policy for Suppliers is required.

For additional requirements please refer to Section 20, *Business-to-Business Connectivity* in LegalMaps' LegalMaps Security Standards document.

7.2.1 Identification of Risks from Third Party Access

Before access is granted to any third party requesting external connectivity, all risks of such connectivity must be evaluated and documented for the system that is to be accessed by such third parties.

7.2.2 Third Party Handling of Customer or LegalMaps Information

7.2.2.1 No third party services pertaining to the electronic handling of customer or LegalMaps information will be solicited or obtained without the written approval of the Director of Information Security of LegalMaps.

7.2.2.2 No third party services pertaining to the electronic handling of customer or LegalMaps information may be activated without the written approval of the Director of Information Security of LegalMaps.

7.2.3 Requirements for Third Party Services & Access

Third parties must provide for secure transmission of LegalMaps data no matter the form.

7.2.3.1 Logical connectivity to Corporate Information Systems by third parties must employ the use of network traffic filtering firewalls for static connectivity, i.e. virtual circuits, leased line, static VPN.

7.2.3.2 Logical connectivity to the Corporate Information Systems by third parties through dynamic, (i.e., Infrequent or temporary connectivity to corporate networks remotely) remote access must be conducted through an approved connection.

7.2.3.3 Legacy dynamic access via directly attached modems must follow guidelines set within for communications security, authentication, access control and third party security and must also receive written approval prior to granting third party access.

7.2.3.4 Logical connectivity to the Corporate Information Systems by third parties through static remote access must adhere to all requirements for third party access, (i.e. contractual agreements including NDA), plus all other requirements specified within that relate to communications security as specified throughout this policy. Equally, the data classification of the Information System being accessed may require that additional access controls be employed prior to granting remote access by third parties.

7.2.3.5 Physical access to LegalMaps Corporate facilities must follow all physical security requirements of the facility in question for approved temporary or contractual access, i.e. some facilities may process restricted corporate or government information requiring all persons with physical access to complete a background investigation prior to access.

7.2.3.6 Maintain responsibility for the connectivity, up to and including the network demarcation point. The demarcation point will be the LAN interface on the most distant LegalMaps router at which the Client Company connects.

7.2.3.7 Network Address Translation (NAT) shall be utilized to conceal internal network addressing.

7.2.3.8 No internal routing information shall traverse the link between companies. Routing shall be achieved through the use of static routes or dynamic routing protocols that advertise public addresses only.

7.2.3.9 All access must be monitored in compliance with all requirements set forth in *Section 7.11.3. Monitoring System Use*, through the use of network device logging and/or intrusion detection/prevention monitors.

7.2.4 Types of Access

The type of access allowed to third parties should be explicit within written contractual agreements and associated security planning addendums.

Types of access that are to be considered are:

1. Physical access, e.g. to offices, computer rooms, and filing cabinets;
2. Logical access, e.g. to an organization's databases, and Information Systems. Two types of logical access exist as follows:
    - Dynamic access, e.g. infrequent or temporary logical access
    - Static access, e.g. permanent or long-term logical access

7.2.5 On-site Contractors and Temporary Employees

Third parties that are located on-site for a period of time as defined in their contract may also give rise to security weaknesses. Examples of on-site third party include:

a. Hardware and software maintenance and support staff
b. Cleaning, catering, security officers and other outsourced support services
c. Student placement and other casual short-term appointments
d. Consultants and temporary employees

It is essential to understand what controls are needed to administer third party access to information processing facilities. Generally, all security requirements resulting from third party access or internal controls should be reflected by a third party contract.

Access to information and information processing facilities by third parties must not be provided until a contract has been signed defining the terms for the connection or access.

Please refer to LegalMaps' LegalMaps Security Standards document, Section 3 *External Access* for further details.

7.3 Third Party Service Delivery

Third party service provider contracts must be obtained through approved LegalMaps procurement channels according to established policies and procedures. All contracts with third party service providers must be reviewed with the Legal department prior to execution. If customer data is shared with the third party, contract language that specifically addresses applicable laws and regulations must be included in the contract. Compliance with the LegalMaps Security Policy for Suppliers is required.

7.3.1 Third Party Software Used for Critical Business Functions

Where third party software will be used to perform critical business functions, the source code must be either licensed to and in the custody of LegalMaps, or the third party must periodically provide source code to a third party agent who will hold the source code in escrow. This policy does not apply to commercial off-the-shelf software.

7.3.2 Additional Items for Third Party Service Agreement

The following terms should be generally included in the contract:

a. Security policy requirements specific to the type of access to be granted;
b. Non-Disclosure Agreement (NDA);
c. Asset protection, including:
    1. Procedures to protect organizational assets, including information and software;
    2. Procedures to determine whether any compromise of the assets, e.g. loss or modification of data, has occurred;
    3. Controls to provide for the return or destruction of information and assets at the end of, or at an agreed point in time during, the contract;
    4. Integrity and availability, including How the availability of services is to be maintained in the event of a disaster;
    5. Restrictions on copying and disclosing information;
    6. A description of each service to be made available;
d. The target level of service;
e. Provision for the transfer of staff where appropriate;

f. The respective liabilities of the parties to the agreement;
g. Intellectual Property Rights, copyright assignment and protection of any collaborative work;
h. Access control agreements, covering:
    1. Permitted access methods, and the control and use of unique identifiers;
    2. An authorization process for user access and privileges;
    3. A requirement to maintain a list of individuals authorized to use the services being made available and what their rights and privileges are with respect to such use;
i. The definition of verifiable performance criteria, their monitoring and reporting;
j. The right to monitor and revoke user activity;
k. The right to audit contractual responsibilities and security posture or to have those audits carried out by a third party in respect to both the third party and LegalMaps itself;
l. The establishment of an escalation process for problem resolution; contingency arrangements should also be considered where appropriate;
m. A clear and specified process of change management;
n. Any required physical protection controls and mechanisms to provide for controls being followed;
o. Controls to provide for protection against malicious software (see *Section 7.5, Protection Against Malicious and Mobile Code);*
p. What levels of physical security are to be provided for outsourced equipment;
q. What arrangements will be in place to establish that all parties involved in the outsourcing, including subcontractors, are aware of their security responsibilities;
r. How the integrity and confidentiality of the LegalMaps business assets are to be maintained and tested;
s. Arrangements for reporting, notification and investigation of security incidents and security breaches; and
t. Involvement of the third party with subcontractors.
u. Compliance with the LegalMaps Security Policy for Suppliers.

7.3.3 Non-Disclosure Agreement (NDA)

Sensitive information must not be shared with any third party unless an LegalMaps approved non-disclosure agreement is in place.

No user shall sign, on behalf of LegalMaps, a non-disclosure agreement presented by a third party without prior appropriate Legal review and approval.

7.3.4 Monitoring and Review of Third Party Services

LegalMaps Security will periodically review the adequacy of third party security controls to confirm that LegalMaps information is properly secured. The frequency of these reviews will be based on criticality and risk of the services provided.

7.3.5 Manage Changes to the Third Party Services

Upon renewal or breach of third party agreements, LegalMaps shall review and update contracts to facilitate the security of customer or LegalMaps information.

7.4 System Planning and Acceptance

Advance planning and preparation are required to provide for the availability of adequate capacity and resources. Projections of future capacity requirements should be made, to reduce the risk of system overload. The

operational requirements of new systems must be established, documented and tested prior to their acceptance and use through Risk Assessments.

System planning will address all issues of planning and acceptance and should be completed for all Information Systems upon system implementation or significant modification.

7.4.1 Capacity Planning

Capacity demands for all production Information Systems should be monitored, and projections of future capacity requirements made, such that adequate processing power and storage are available. These projections should take account of new business and system requirements and current and projected trends of the organization's information processing. They should identify trends in usage, particularly in relation to business applications or management Information System tools.

Product and/or technology managers should use this information to identify and avoid potential bottlenecks that might present a threat to system security or user services, and plan appropriate remedial action.

7.4.2 System Acceptance

Acceptance criteria for new Information Systems are established with Risk Assessment documented controls to confirm that appropriate controls have been implemented, reviewed, and properly tested.

The Information System owner is responsible for system acceptance through signed authorization provided within the Information System's Risk Assessment.

7.5 Protection against Malicious & Mobile Code

Software and information processing facilities are vulnerable to the introduction of malicious software, such as computer viruses, network worms, Trojan horses (see also Section 9.6, *Technical Vulnerability Management*), and logic bombs.

Detection and prevention controls to protect against malicious software, and appropriate user awareness procedures, shall be implemented. Protection against malicious code is based on a combination of factors including security awareness training, appropriate system access, and change management controls.

7.5.1 Controls against Malicious & Mobile Code

The following controls are required for all LegalMaps Information Systems (where technologically feasible):

7.5.1.1 LegalMaps Security approved anti-virus software must be implemented by LegalMaps on all PCs, servers, laptops, PDAs, or other devices capable of being a host for viruses, worms, or other forms of malicious code. The software must be the LegalMaps Security approved version and must use a standard LegalMaps Security approved configuration and signature file update scheme. Please refer to LegalMaps' LegalMaps Security Standards document for more details regarding antivirus requirements.

7.5.1.2 Electronic files capable of hosting malicious code must be scanned for viruses via a LegalMaps approved method before being introduced into LegalMaps's computer environment. This includes, but is not limited to, program and executable files, data files, e-mails, e-mail attachments, and electronic documents and spreadsheets.

7.5.1.3 LegalMaps users must not take any action that will disable or hinder the operation of anti-virus software or to alter the configuration of the software.

7.5.1.4 LegalMaps users must promptly report the detection of any computer virus or malicious code to the LegalMaps Help Desk.

7.5.1.5 LegalMaps users are prohibited from installing, operating, or downloading any unauthorized or unlicensed software, shareware, or freeware from any source utilizing LegalMaps Resources. For example, users must not accept offers to automatically install software from the Internet or self-install demonstration software received in the mail or from a seminar.

7.5.1.6 LegalMaps users must not intentionally write, generate, compile, copy, propagate, execute, or attempt to introduce any computer code (i.e., virus, worm, or malicious code) designed to self-replicate, damage, or otherwise hinder the performance of any computer, network, software, or system.

7.5.1.7 A master copy of all personal computer and server software must exist, and such copies must be stored in a secure location. These master copies must not be used for ordinary business activities but must be reserved for recovery from computer virus infections, hard disk crashes, and other computer problems in accordance to the Business Continuity Plan.

7.5.1.8 Procedures to verify all information relating to malicious software and to confirm that warning bulletins are accurate and informative shall be established. Users should be made aware of the problem of hoaxes and what to do upon receipt of them.

7.5.1.9 Misuse of Software

All end user use of software on LegalMaps Information Systems must be authorized for use prior to implementation. Authorization requires LegalMaps Security coordination with supporting business units prior to use.

In regards to software licensed by LegalMaps, users may not do any of the following without prior authorization:

a. Copy software for use on their home computers
b. Provide copies of software to any independent contractors or clients of LegalMaps or to any third party
c. Install software on any of LegalMaps' workstations or servers
d. Download any software from the Internet or other online service to any of LegalMaps' workstations or servers
e. Modify, revise, transform, recast or adapt any software
f. Reverse-engineer, disassemble or decompile any software.

Users who become aware of any misuse of software or violation of copyright law should immediately report the incident to their supervisors.

For additional requirements please refer to LegalMaps' LegalMaps Security Standards document.

7.6 Back-Up

Reasonable and effective steps must be taken such that data or software resident on all computer systems and file servers are backed-up appropriately based on the nature and volatility of the data or software they contain.

7.6.1 Information Back-Up

Back-up data must be afforded the same level of security as the original data.

7.6.2 Procedures for Critical Information

Procedures must exist to enforce the requirement that critical information can be recovered to a known consistent state in the event of a system failure or corruption.

7.6.3 Backups to Facilitate Business Continuity

Back-ups necessary to facilitate business continuity must be stored in an environmentally protected and access-controlled site separate from the LegalMaps location where the source data resides. Non-business continuity related back-ups (i.e., end user performed back-ups) must be stored in a secure manner.

7.6.4 Recovered or Restored Data

Recovered data or data restored from back-up must be afforded the same level of security as was intended for the original data.

Applicable references to this section may be found in Section 11, Business Continuity Management.

7.7 Network Security Management

The management of networks should be tightly controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

7.7.1 Network Controls

A range of controls is required to achieve and maintain security in computer networks. Network managers should implement controls to manage the security of data in networks and the protection of connected services from unauthorized access.

7.7.1.1 Systems must not establish communications in order to send or receive data unless authentication and authorization are mutually assured between the sender and the receiver. System-level communications, such as those necessary to establish identity or network availability without requiring authentication, are excluded from this policy.

7.7.1.2 Any service or operational entity not under the direct management of LegalMaps or its authorized delegate must be isolated from the LegalMaps network by a firewall and/or other appropriate means approved by LegalMaps Security.

7.7.1.3 All LegalMaps networks must be configured and enabled via LegalMaps Security-approved means such that they can prevent and/or detect attempts to establish unauthorized connections or make unauthorized entry.

7.7.1.4 All LegalMaps network devices (routers, firewalls, access control servers, etc.) must have access control mechanisms and a security configuration approved by LegalMaps Security.

7.7.1.5 All vendor-supplied default passwords must be changed before any computer or communications system is used for LegalMaps business.

7.7.1.6 All inbound dial-up, DSL and cable modem connections to LegalMaps' network must require two levels of user authentication when accessing Confidential or Highly-Restricted information. This authentication may include callback devices, dynamic password software, identity tokens, or other methods approved by LegalMaps Security in writing.

7.7.1.7 Users must not establish electronic bulletin boards, local area networks, FTP servers, wireless data transceivers, web servers, modem connections to LegalMaps networks or external networks, or other multi-user systems unless approved through authorized LegalMaps Security channels.

7.7.1.8 No non-LegalMaps device may be directly connected to the LegalMaps network or systems without an approved Security Exception.

7.7.1.9 Users are prohibited from installing or contracting with third parties for the installation of modem lines or other telecommunications facilities that connect to LegalMaps computers or networks without an approved Security Exception.

7.7.1.10 Operational responsibility for networks should be separated from computer operations where possible (see Section 7.1.3, *Segregation of Duties*).

7.7.1.11 Authentication must be implemented on all systems enabling access to a system or network.

7.7.1.12 Authorization mechanisms must be implemented and maintained at all times.

7.7.1.13 Controls must be implemented on all systems to support the requirement that data cannot been altered or modified in any way except as permitted by authorized parties.

7.7.1.14 Separation of sensitive information or resources classified as Confidential or Highly Restrictive: sensitive resources or applications containing sensitive information should run on isolated environments via logically or physically dedicated systems.

7.7.1.15 Segregation: Large networks should be segregated based on the classification and where sensitive information resides. A multi-tiered infrastructure is required for all systems that store, process, or transmit sensitive information. For details of proper segregation and separation of sensitive systems, please see Section 8.4.9, *Network Routing Control (Gateways/Firewalls).*

7.7.1.16 Production networks must logically be segregated.

7.7.1.17 Monitoring and Management Systems should be separated from other systems, and administrative access to these systems must utilize approved encryption and adhere to all requirements for authentication.

7.7.1.18 Network Routing Controls: Ingress and egress controls must be applied to protect data passing over non-LegalMaps networks (spoof prevention) to support the requirement that source and destination addresses are positively identified and enforced.

7.7.1.19 Network Operations responsibilities should be defined and separate from computer operations where possible. Network Operations will also be responsible for documenting the network and any systems accessible from the network.

7.7.2 Security of Network Services

For any in-house or outsourced network agreement, LegalMaps must confirm that security features, service levels, and management requirements are identified and included in all agreements in accordance with this policy.

7.8 Media Handling

Media should be controlled and physically protected based on the classification of the Information System in question. See Section 4, *Asset Management* for additional details.

Appropriate operating procedures should be established by data owners/custodians to protect documents, computer media (tapes, disks, and cassettes), input/output data and system documentation from damage, theft and unauthorized access.

7.8.1 Management of Removable Media

Procedures for the management of removable computer media, such as tapes, disks, cassettes and printed reports shall be developed and implemented by technology managers in conjunction with this policy. Specific policies for media handling are defined as a part of data classification and are specific to the Information System in question; please see Section 4, *Asset Management* for more information. The following controls are required:

7.8.1.1 Authorization is required for all media removed from the organization and a record of all such removals to maintain an audit trail is to be kept.

7.8.1.2 A procedure to check-out or remove media from operational areas is required.

7.8.1.3 **Highly-Restricted** information, no matter the form, cannot be removed from any LegalMaps premises without the advance approval of the LegalMaps Director of Information Security.

7.8.1.4 **Consumer** information, no matter the form, must not be removed from any LegalMaps premises without the advance approval of Security Investigations and Credentialing.

7.8.1.5 All media, whether at a LegalMaps location or third party, will be stored in a safe, secure environment, in accordance with manufacturers' specifications and this policy.

7.8.1.6 Media, no matter the form, may not be shipped or transmitted to another country without permission from the LegalMaps Director of Information Security.

7.8.1.7 A current inventory of all tape backup media, whether the backup media is kept onsite or at a remote site, must be maintained and reviewed at least annually.

7.8.2 Disposal of Media

All LegalMaps information must be destroyed when it is no longer needed or its retention period has passed. All media that contains information or is output from an Information Resource should be disposed of securely and safely. Media may include, but is not limited to: hard drives, disks, paper, film, microfiche, tapes, diskettes, USB drives, or other destroyable electronic, digital, or physical media.

Disposal of media is the responsibility of LegalMaps or an approved vendor. Please refer to LegalMaps' LegalMaps Security Standards document, Section 22, *Security Standards for Media Sanitizing/Disposal* for additional information.

Formal media disposal procedures shall include (at a minimum):

7.8.2.1 Media awaiting destruction shall be secure at all times.

7.8.2.2 Identifying a list of media types that require secure disposal, such as paper documents, voice or other recordings, carbon papers, reports output from Information Resources, printer or typewriter ribbons, magnetic tapes, optical storage media, removable media or cassettes, system documentation, test data, etc.

7.8.2.3 A central secure disposal collection site should be clearly marked in each office so that associates can deliver the media to be securely disposed of (in this case an office administrator would coordinate the disposal of media after it has been collected).

7.8.2.4 Any third-party or contracted media disposal services should be carefully selected. Only reputable service providers should be used. The service provider will come on-site to perform the disposal.

7.8.2.5 Disposal of any media containing LegalMaps-HIGHLY RESTRICTED information (see Section 4.4, *Information Labeling and Handling Requirements* for more information) should be logged when disposed of. The log should include the associate disposing of the media, a description of the information contained within the media, and the date and time of the disposal.

7.8.2.6 Shredding is the only approved method for physical destruction. Media to be destroyed shall be immediately shredded or placed in locked bins.

7.8.2.6.1 Facility managers shall provide for a sufficient number and proper location of locked storage bins to support their proper use.

7.8.2.6.2 Access to keys for unlocking bins shall be restricted to authorized personal determined by Global Physical Security.

7.8.2.6.3 Locked bins will be kept inside facilities until the contents are shredded.

7.8.2.6.4 An LegalMaps user must witness the locked bin contents being shredded onsite at an LegalMaps facility prior to signing a certificate for the number of bins shredded.

7.8.2.6.5 A certificate from a contracted shredding company must be received for all storage bins that are processed for shredding.

7.8.2.6.6 Locations where locked bins do not exist, users are responsible for destroying material immediately or no later than by close of business via personally managed shredders.

7.8.3 Information Handling Procedures

Procedures for the handling and storage of information shall be established in order to protect such information from unauthorized disclosure or misuse. Procedures should be drawn up for handling information consistent with its classification (see Section 4.3, *Information Classification*).The following controls are required:

7.8.3.1 Highly-Restricted information in hardcopy (paper) form may only be sent by trusted courier. Regular or restricted mail is prohibited.

7.8.3.2 Highly-Restricted information may not be discussed or displayed in public.

7.8.3.3 Highly-Restricted information may not be sent to an unattended fax machine unless the destination machine is in a locked room.

7.8.3.4 If Highly-Restricted information is released orally in a meeting, the speaker must communicate the sensitivity of the information beforehand.

7.8.3.5 Handling and labeling of all media is required.

7.8.3.6 Access restrictions to identify unauthorized personnel are required.

7.8.3.7 Maintenance of a formal record of the authorized recipients of data is required.

7.8.3.8 Storage of media in an environment which accords with manufacturers' specifications.

7.8.3.9 Clear marking of all copies of data for the attention of the authorized recipient; review of distribution lists and lists of authorized recipients at regular intervals consistent with its classification as seen in Section 4.3, *Information Classification*.

7.8.4 Security of System Documentation

System documentation may contain a range of sensitive information, e.g. descriptions of applications processes, procedures, data structures, and authorization processes. The following controls are required to protect system documentation from unauthorized access:

7.8.4.1 System documentation should be stored securely in an approved, locked container.

7.8.4.2 The access list for system documentation should be kept to a minimum and authorized by the application owner.

7.8.4.3 System documentation held on a public network, or supplied via a public network, should be appropriately protected.

7.9 Exchange of Information

LegalMaps recognizes that information can be vulnerable to unauthorized access, misuse or corruption during physical transport, for instance when sending media via the postal service or via courier.

7.9.1 Information Exchange Policies & Procedures

Exchanges of information and software between organizations should be controlled, and should be compliant with relevant legislation.

7.9.2 Exchange Agreements

Exchanges should be carried out on the basis of agreements. Procedures and standards to protect information and media in transit shall be established. The business and security implications associated with electronic data interchange, electronic commerce and electronic mail and the requirements for controls should be considered.

7.9.3 Physical Media in Transit

The following controls shall be applied to safeguard physical computer media being transported between sites or vendors:

7.9.3.1 Any data that cannot be encrypted per LegalMaps' LegalMaps Security Standards must be shipped using an armed courier service that has been approved by LegalMaps Security.

7.9.3.2 Reliable transport or couriers should be used. A list of authorized couriers should be agreed with management and a procedure to check the identification of couriers implemented.

7.9.3.3 Packaging should be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with manufacturers' specifications.

7.9.3.4 Special controls should be adopted, where necessary, to protect sensitive information from unauthorized disclosure or modification. Examples include the use of locked containers, tamper-evident packaging, and delivery by hand.

7.9.4 Electronic Messaging & Data Transmissions

Digital information in transit requires special attention paid to the media used for transit and the information to be transmitted. The following controls have been established and are required for data in transit:

7.9.4.1 Encryption shall be used for transmitting sensitive information (Class 3 or above) over public networks among LegalMaps facilities and between LegalMaps and other facilities or third parties. This includes, but is not limited to file transfers, email, and messaging systems.

7.9.4.2 The encryption methodology used must be approved by LegalMaps Security.

7.9.4.3 Strong authentication (as defined in Section 8.3.2, *Strong Authentication*) must be used for transmitting sensitive information (Class 3 or above) over all networks among LegalMaps facilities and between LegalMaps and other facilities or third parties.

7.9.4.4 Sensitive information in transit over private communication lines such as a frame-relay or point-to-point circuit must be encrypted. An encrypted electronic transmission solution shall be implemented by 12/31/2009 on all existing frame-relay and point-to-point circuits and does not require an exception until such time. The type of information in transit may fall under additional requirements for encryption based on its classification or function, i.e. Database or system administration or database information with a classification of Class 3 or above. See Section 7.13 *Encryption Requirements* for more information.

7.9.5 Security of Electronic Mail and Messaging

Email is one of our most important methods of communicating with each other and with our clients, customers, vendors, and consultants. To maximize the benefits of this medium and minimize potential liability, LegalMaps has created the following guidelines:

7.9.5.1 Information Systems hosting corporate email services, by default, fall under the classification of Confidential (Class 3), at a minimum, and must be protected in accordance with classification. Individual messages held by such systems remain individually classified for the purpose of sending and receiving messages in relation to security compliance. See Chapter 4, *Asset Management*.

7.9.5.2 Electronic mail transiting between LegalMaps locations must not travel over public networks unless protection of sensitive information has been established as per requirements of data in transit as specified by this policy. See Section 7.9.7, *Security Requirements for Messaging Systems* for details.

7.9.5.3 Email transiting from the Internet or external systems to corporate email subscribers must be searched for malicious code and viruses at all Internet email gateways. E-mail gateways must have installed and running an up-to-date version of antivirus software. Anti-virus software on email gateways must be updated within two hours of the release of a new signature file update.

7.9.5.4 Corporate personnel sending or receiving e-mail via the Internet or other external systems must be identified and authenticated. All email sent to or from corporate email subscribers via the Internet or other external systems must be logged. The capability must exist for logged e-mail and attachments to be rapidly keyword searched.

7.9.5.5 This footer must be appended to all email sent outside LegalMaps by the mail gateway:

The information contained in this message may be proprietary and/or confidential, and protected from disclosure. If the reader of this message is not the intended recipient, or an employee or agent responsible for delivering this message to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify LegalMaps immediately by replying to the message and deleting it from your computer.

7.9.6 Electronic Mail User Requirements

In using the e-mail system, all users must comply with the following guidelines:

7.9.6.1 E-mail systems may not be used for any type of solicitation other than those directly related to business activities. This restriction includes, but is not limited to any religious, political, charitable, social, or personal purposes.

7.9.6.2 E-mail users will not send or disclose LegalMaps confidential or sensitive information to anyone without the need to know. Under no circumstances will the use of unencrypted Internet e-mail be used to send any LegalMaps sensitive information to any persons.

7.9.6.3 Sensitive information or files being transmitted by email to a destination outside of LegalMaps should be encrypted by approved means as specified in LegalMaps' LegalMaps Security Standards document, Section 11, Encryption/Cryptography Requirements.

7.9.6.4 Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate may not be created, sent, or forwarded by email. If a user encounters this kind of material, they are obligated to report it to their supervisor.

7.9.6.5 Chain e-mail is a non-business related message sent to a number of people asking each recipient to send copies with the same message to a specified number of others. Users should delete all chain e-mail and all non-business-related mass email immediately upon receipt and refrain from forwarding to any other users.

7.9.6.6 Never alter the "From:" line or other attribute-of-origin information in e-mail. Anonymous or pseudonymous messages are forbidden.

Please refer to LegalMaps' LegalMaps Security Standards document, Section 5: Security Standards for Messaging for further details.

7.9.7 Security Requirements for Messaging and Web Conferencing Systems

Chat, instant messaging, web conferencing, and all other forms of digital communication over public networks are not allowed for corporate use unless supported internally. Transmission of corporate information over public networks is not allowed unless it can be appropriately secured through acceptable forms of encryption; see Section 7.9.5, *Security of Data Transmissions* and Section 7.5, Protection Against Malicious and Mobile Code for acceptable use of software on corporate Information Systems. Use of internal video conferencing solutions (web cams and video conferencing software) is also allowed as long as the activity is for business purposes only, occurs outside of rooms or areas where sensitive information or systems are located, and as long as corporate-approved hardware and software are used.

Messaging systems must adhere to the following requirements:

7.9.7.1 All systems/connections used to transport corporate messages must be approved prior to systems/connections becoming operational. An up-to-date inventory of all approved systems/connections must be maintained. Only approved systems/connections are permitted.

7.9.7.2 All systems/connections to the Internet or other external systems that transport corporate messaging should be real-time monitored and controlled so that any changes in the status of systems/connections are detected and managed.

7.9.7.3 Messages transiting from the Internet or external systems to corporate messaging subscribers must be searched for malicious code and viruses at all Internet messaging gateways. Messaging gateways must have installed and running an up-to-date version of anti-virus software. Anti-virus software on messaging gateways must be updated within two hours of the release of a new update.

7.9.7.4 Corporate personnel sending or receiving messages via Internet or other external systems must be identified and authenticated. All messages sent to or from corporate messaging subscribers via the Internet or other external systems must be logged to provide a ninety (90) day audit trail of both inbound and outbound messaging traffic. The capability must exist for logged messages and attachments to be rapidly keyword searched.

7.9.7.5 In the event a security breach of LegalMaps' messaging systems/connections is detected, staff must implement the incident response plan. This incident response plan includes notifications, points-of-contact, back-up procedures, and all relevant actions that are required to recover from an incident.

7.9.7.6 Testing to validate the sufficiency of messaging security controls should be conducted at least monthly. Messaging systems/connections must employ the latest security patches, anti-virus software, and be capable of identifying any changes to existing configurations.

7.9.8 Business Information Systems

Encryption is required for transmission of sensitive or transactional information over all Public Information Systems to be in compliance with this policy.

7.9.9 Additional Communications Encryption Requirements

Communications encryption refers to active communications to Information Systems and associated applications, including database access. (i.e. Intra/Internet sites, systems administration applications, web to application server, etc.)

All applications must utilize encryption for the transmission of user credentials, passwords, financial and personally identifiable information and all other information protected by privacy and security regulations.

Communications Encryption Matrix

	Unrestricted (Class 1)	Internal (Class 2)	Confidential (Class 3)	Highly Restricted (Class 4)
Application Access	No	No	Yes	Yes
Systems Administration	Yes	Yes	Yes	Yes

cifics on encryption requirements and approved protocols can be found in Section 7.13, *Encryption Requirements* as well as LegalMaps' LegalMaps Security Standards document, Section 11, Encryption / Cryptography.

ems Administration is defined as non-console access to Information Systems technology for the purpose of remotely managing the technical resource. Encryption of the data stream and its contents are always required.

7.10 Electronic Commerce Services

Electronic commerce can involve the use of electronic data interchange (EDI), electronic mail and online transactions across data networks between third parties.

7.10.1 Electronic Commerce & On-Line Transactions

Electronic commerce Security requirements for electronic commence should include the following controls:

7.10.1.1 Authentication. All access to information classified as Class 2 or above must be authenticated by means of, at a minimum, username and password adherent to authentication requirements specified herein.

7.10.1.2 Authorization. Authorization must be provided in a discretionary form and role based permissions, supporting the requirement that only those with a need-to-know have access to the information in question.

7.10.1.3 Accountability. All authorized access to information classified as Class 2 or above must include, where systems can accommodate appropriate controls required to audit access to the information in question. Event logging, where systems can accommodate must be inclusive enough to be able to reconstruct any event in time accurately, and in a timely fashion, in order to identify malicious activity for the purpose of forensic investigation.

7.10.1.4 Contract and Tendering Processes. For Internal Use Only forms of access, i.e. access between businesses or partners requiring contractual agreements, all access must be documented, contracted, and reviewed annually.

7.10.1.5 Order Transactions. Confidentiality and privacy statements, integrity of order, payment and delivery address verification, and confirmation of receipt (if possible) must be provided as a part of the application design.

7.10.1.6 Vetting. Vetting, or inspection of information, provided for financial transactions must be verified through reasonable means such that payment methods and associated purchaser are valid prior to accepting payment for any services or products.

7.10.1.7 Ordering. Protection of ordering must be provided through approved means of encryption, integrity and confidentiality controls, means of non-repudiation, and equivalent privacy statements.

7.10.1.8 Liability. Liability for fraudulent transactions must be identified and details of such terms of liability must be available to any individual conducting financial transactions.

Many of the above considerations can be addressed by the application of cryptographic techniques outlined in Section 9.3, *Cryptographic Controls*, taking into account compliance with legal requirements, *Section 12.1 Compliance with Legal Requirements*.

7.10.2 Supplementary Storage Requirements for Cardholder Data per Payment Card Industry (PCI) Security Standards

Do not store sensitive authorization data (such as track data) after transaction authorization is complete, per Payment Card Industry security requirements. A mechanism must be implemented to logically segregate each merchant's stored cardholder data.

7.10.3 Security of Domain Name Services

Security of Domain Name Services (DNS) is critical to the support of all Information Systems since exposure of private naming and addressing could allow for simplified infrastructure mapping and potential compromise. The following policies apply to all LegalMaps Domain Name Services:

7.10.3.1 LegalMaps DNS servers must be configured to disallow zone transfers to unauthorized hosts.

7.10.3.2 External DNS servers may only serve information that is publicly available, i.e. internal addresses and internal naming conventions are not allowed to pass to public networks. Authorized third party connections are excepted if such connections are privatized by use of private lines or VPN.

7.10.3.3 Firewalls must filter traffic to and from external DNS servers for only UDP Port 53 unless authorized zone transfers are in effect. Authorized zone transfers must be restricted to TCP and UDP Port 53 between only those authorized zone transfer hosts. This shall be performed through access control lists.

7.10.4 Publicly Available Information

The integrity and availability of publicly available information must be verified and test controls implemented to protect LegalMaps' reputation and standing in the consumer and business community.

7.10.4.1 Press releases must be approved through Corporate Communications before being issued.

7.10.4.2 Internet-facing web site content must also be approved by Corporate Communications before publication.

7.10.5 Other Forms of Information Exchange

Procedures and controls are required to protect the exchange of information through the use of voice, facsimile and video communications facilities. Information could be compromised due to lack of awareness, policy or procedures on the use of such facilities.

Care must be taken when utilizing voice, fax, or video communications. It is the responsibility of LegalMaps Security personnel through Security Awareness Training and peer interactions to remind others to take precautions when communicating over voice, fax and video that eavesdropping and interception are likely.

7.11 Monitoring

System and policy monitoring allows the effectiveness of controls adopted to be checked and conformity to an access policy model to be verified. System monitoring is required for all LegalMaps Information Systems, and network segments with public exposure.

7.11.1 Intrusion Detection/Prevention Requirements

The following requirements pertain to all intrusion detection/prevention operations:

7.11.1.1 Operating systems will be monitored to detect deviation from access control policy and record events to provide evidence in case of security incidents.

7.11.1.2 Network segments with direct public exposure, i.e. Internet exposure requires the use of network intrusion detection/prevention services capable of detecting and reporting potential malicious activities and relevant events that could affect the security of the organization or its customers.

7.11.1.3 Sensitive Information Systems, and their associated operating systems, with a classification level of Confidential (Class 3) or above require the use of host-based intrusion detection/prevention software and/or hardware and policy monitoring software capable of detecting and reporting local policy changes.

7.11.1.4 All intrusion detection/prevention must be centrally monitored at the designated corporate facility and centrally controlled by the local business unit so that any changes in the status of their security, as well as the corporate systems being monitored, is detected and managed.

7.11.1.5 Testing to validate the sufficiency of staff actions as it pertains to incident handling should be tested frequently, with duration of no less than annually.

7.11.1.6 Responding to incidents in accordance with policies for security incidents and malfunctions as described in Section 10.1, *Reporting Security Events*.

7.11.1.7 Retention requirements for Intrusion Monitoring must follow guidelines for data retention set forth in Section 4.5, *Corporate Retention Requirements*.

7.11.1.8 All intrusion detection/prevention controls must be properly maintained and sufficiently updated with signatures, patches, and other appropriate updates as detailed in Section 9.6.1, *Patch Management*.

7.11.1.9 Testing to validate the sufficiency of staff actions as it pertains to the response handling of Severity Level 1, 2, and 3 alerts must be conducted at least quarterly. See Section 10.2.2, *Classification of Alert Severity Levels*.

7.11.1.10 Intrusion Detection/Prevention systems must provide for the following capabilities:

Threat Management: Real-time management of security threats, intrusions and policy violations.

Analysis: Provide a solution for the historical analysis of intrusion detection/prevention logs enabling queries and analysis of logs from a central location.

Information Captured: Capture of the IP address of the source and destination of the activity, timestamps, alert names, event data, as well as the names of the related files and objects that were grounds for the alert is mandatory. Capture of User ID's, MAC addresses, process ID's, event IDs, and other appropriate information if it is available for capture.

Automation: Mitigate high-risk threats through the automation of key security processes and alerts.

Reporting: Report security threats, intrusions, and policy violations from a central location at the local business unit for local reporting and from the designated corporate facility for corporate-wide reporting.

7.11.1.11 Intrusion Monitoring Guide Table

The following table represents the requirements for intrusion monitoring based on the classification of the Information System. Intrusion monitoring in all forms is required, but not limited to, any LegalMaps Information System that stores, processes, or transmits information classified as LegalMaps Confidential (Class 3) or greater.

	Public (Class 1)	Internal Use Only (Class 2)	Confidential (Class 3)	Restricted (Class 4)
Network Intrusion				
Host Intrusion	No	No*	Yes	Yes
Policy Monitoring	No	No*	Yes	Yes

* Highly recommended, but not required unless such systems have direct connectivity to Information Systems classified as Class 3 or above.

7.11.2 Audit Logging

Network resources and databases handling sensitive information must be configured to log all significant successful and unsuccessful computer security events as defined by LegalMaps Security to aid in monitoring compliance with security measures. These audit logs must be reviewed by LegalMaps Security or an approved delegate for suspicious or unauthorized activity. These audit logs must be retained by LegalMaps Security or an approved delegate as defined in applicable standards and procedures.

The accepted LegalMaps policy for event logging is intended to support the requirement that system data is captured and archived. The following is at a minimum to be logged:

- User ID; source IP address, destination IP address, protocol, and port, if applicable;
- Dates and times for successful and unsuccessful (failed) logon attempts;
- Application of patches;
- Changes in privilege user rights.

Event or Audit Log reviews should be done in accordance with the separation of duties to avoid a single area of responsibility. The logging facility should be designed with the following:

- Logging facilities should be designed to prevent tampering;
- Logging facilities should record deactivation events if de-activation is possible;
- Logging facilities should record event or log-file deletion.

7.11.2.1 Systems Logging Review

Systems Logging refers to the frequency of administrative review of active/archived system logs to be conducted by the administrator for the system or devices within the classified Information System.

	Public (Class 1)	Internal Use Only (Class 2)	Confidential (Class 3)	Restricted (Class 4)
Operating System and Application Security Logs	Monthly	Semi-Monthly	Weekly	Daily

7.11.3 Monitoring System Use

Procedures for monitoring the use of information processing facilities should be established. Such procedures are necessary to support the requirement that users are only performing activities that have been explicitly authorized. The level of monitoring required for individual facilities should be determined by a risk assessment. Areas that should be considered include:

a. Authorized access, including detail such as:
    1. The user ID;
    2. The date and time of key events;
    3. The types of events;
    4. Origination point of the event (i.e. IP address, user or station name, etc.)
    5. The files accessed; and
    6. The program/utilities used.
b. All privileged operations, such as:
    1. Use of supervisor account;

2. System start-up and stop;
3. I/O device attachment/detachment;
4. Initialization of the audit log file.

c. Unauthorized access attempts, such as:
   1. Failed attempts;
   2. Access policy violations and notifications for network gateways and firewalls;
   3. System alerts or failures such as:
      i. Console alerts or messages;
      ii. System log exceptions; and
      iii. Network management alarms.

d. File integrity monitoring of critical system files.

7.11.4 Protection of Log Information

Logging facilities and log information shall be housed in a central repository that will be secured to prevent unauthorized tampering and unauthorized access.

7.11.5 Administrator and Operator Logs

All administrator, root, and system operator successful and unsuccessful activities shall be logged and monitored.

7.11.6 Fault Logging

All operations systems faults shall be logged, analyzed, and appropriate action taken to stop or prevent an operations system from failure, unauthorized use or access.

7.11.7 Clock Synchronization

Time consistency should be assured for all systems and devices. The use of clock synchronization systems should be used such that all systems have consistent times. The correct setting of computer clocks is important to provide for the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidence.

Where a computer or communications device has the capability to operate a real-time clock, it should be set to an agreed standard, e.g. Universal Coordinated Time (UCT) or local standard time. Some clocks are known to drift with time. There should be a procedure that checks for and corrects any significant variation.

The Network Time Protocol (NTP) provides a mechanism to synchronize time on computers across an internet. The specification for NTP version 3 is defined in RFC 1305 and is referred to as Extended Network Time Protocol (XNTP).

All Information Systems specified and separated by Risk Assessment documentation must synchronize time with an internal trusted time source such that all systems within the processing entity in question are synchronized with each other.

The Network Engineering Group is responsible for all corporate time services; please seek advice prior to setting time protocols as LegalMaps has established an internal time synchronization method and direct requests to external sources is not allowed.

7.11.8 Time Stamp

Each logged event must be associated with a user, time-stamp and a location or identity of the source used.

7.11.9 Identification & Elimination of Wireless Connectivity

It is the responsibility of LegalMaps Security to periodically arrange tests to identify and eliminate unauthorized wireless connectivity and access points to LegalMaps Information Systems.

7.11.10 Additional Requirements for Wireless Connectivity

7.12.2.1 All wireless connectivity to LegalMaps internal Information System networks falls under all requirements for remote access and strong authentication as specified in Section 8.4.2, *Remote Access*.

7.12.2.3 All wireless technology must utilize approved levels of encryption. See Section 7.13, *Encryption Requirements*.

7.12.2.4 All passwords used in wireless connectivity must adhere to the LegalMaps password policy, *Section 8.3.1, Passwords and PIN Use*.

7.12.2.5 All wireless networks must be centrally monitored for intrusion at all times.

7.12.2.6 Portable Electronic Devices (PED's) with wireless transceivers must be disabled and/or removed unless prior approved for use with or for LegalMaps business. Only LegalMaps owned devices may be used for wireless transmission.

7.12.2.7 LegalMaps Security will maintain an up-to-date inventory of all approved wireless technology systems.

7.12.2.8 Periodically validate the sufficiency of security controls: Testing to validate the sufficiency of security controls for wireless systems must be conducted at least annually by LegalMaps Security. This may be monitored by overlay wireless intrusion monitoring systems.

7.12 Encryption Requirements

Encryption is an important part of secure communications and storage of LegalMaps information.

7.12.1 Encryption Rules to apply to all Sensitive Information Requiring Encryption

7.13.1.1 Encryption during offsite storage, when data is at rest, is required for sensitive fields, but is not required for the whole of databases or network storage unless field level encryption is not possible.

7.13.1.2 Sensitive information in transit, physical or electronic, must be encrypted when not on LegalMaps' network or premises.

7.13.1.3 All administrative communications for the purpose of system or application administration require encryption such as SSH or VPN where the machine/application is capable of receiving such a communication connection.

7.13.1.4 Cryptography shall be implemented in hardware, firmware, software, or a combination thereof. Hardware encryption is preferred and suggested.

7.13.1.5 Highly sensitive information such as passwords, cardholder data, personally identifiable information, and banking information stored offsite must be rendered unreadable by using any of the following approaches:

- One-way ciphers or hashed indexes (such as SHA-1 but not MD5)
- Truncation

- Index tokens and PADs, with the PADs being securely stored
- Strong cryptography, such as Triple-DES or AES with associated key management processes and procedures.

7.13.1.6 Cryptographic solutions must be implemented so that:

- Secret data may not be disclosed
- Conforms to applicable international and national standards, as well as legal and regulatory controls

Please refer to LegalMaps' LegalMaps Security Standards document, Section 10: *Security Standards for Cryptography* for additional details.

7.12.2 Regulation of Cryptographic Controls

Some countries have implemented agreements, laws, regulations or other instruments to control the access to or use of cryptographic controls. Legal advice should be sought to provide for compliance with national law. Before encrypted information or cryptographic controls are moved to another country, legal advice should also be taken.

7.13 Outsourcing

Outsourcing arrangements should address the risks, security controls and procedures for Information Systems, networks and/or desktop environments in a contract between the parties. Compliance with the LegalMaps Security Policy for Suppliers is required

7.13.1 Security Requirements for Third Party Hosting

7.14.1.1 Any LegalMaps assets hosted at a third-party facility must meet all LegalMaps physical security requirements.

7.14.1.2 Any LegalMaps assets hosted at a 3rd party site facility must follow all policies stated herein including the security requirements for Public Information Systems (if publicly exposed) prior to being deployed in a production state.

7.14.1.3 Service Level Agreements (SLA's), outlining how the hosting site will protect and respond to security issues, must be in place.

7.13.2 External Facilities Management

The use of an external contractor to manage information processing facilities may introduce potential security exposures, such as the possibility of compromise, damage, or loss of data at the contractor's site. These risks should be identified in advance, and appropriate controls agreed with the contractor and incorporated into the contract.

Particular issues that should be addressed include:

a. Identifying sensitive or critical applications better retained in-house;
b. Obtaining the approval of business application owners;
c. Implications for business continuity plans;

d. Security standards to be specified, and the process for measuring compliance;

e. Allocation of specific responsibilities and procedures to effectively monitor all security activities;

f. Responsibilities and procedures for reporting and handling security incidents (see Section 10.1 Reporting Security Events.

8 Access Control

Access control is the method by which access to information or sensitive areas of business operations is controlled with the purpose of managing the risk associated with business interruption, information misuse, loss, interruption, or system misuse.

8.1 Access Control Policy

Access is the ability to do something with a resource (e.g., use, change, or view). Access control is the means by which the ability is explicitly enabled or restricted in some way. Computer based access controls can prescribe not only who or what process may have access to a specific system resource, but also the type of access that is permitted. These controls may be implemented in the computer system or in external devices. Access controls must be employed on all LegalMaps Information Systems. Access controls may be reviewed at any time based on business and security requirements for an Information System or physical device.

8.1.1 Access Control Rules

Controlling access to business objects is accomplished through the use and enforcement of access control rules. Access control rules must be written with the philosophy that all access is first denied, unless specifically permitted. Access control rules should be reviewed at least annually and checked for validation, applicability, and practicability. The following requirements apply to all information processing systems that store, process, or transmit information to include at a minimum, computer systems, network devices and security devices:

8.1.1.1 All Information Systems require authentication compliant with all policies herein, whether access is by network, local or even if the system does not have network connectivity. Users must be authenticated and authorized to access LegalMaps systems and data.

8.1.1.2 Do not display system or application identifiers until the log-on process has been successfully completed, with exceptions being network domains.

8.1.1.3 Do not provide help messages during the log-on procedure that would aid an unauthorized user.

8.1.1.4 Validate the log-on information only on completion of all input data. If an error condition arises, the system should not indicate which part of the data is correct or incorrect.

8.1.1.5 Identifying and verifying the identity, and if necessary, the terminal or location of each user;

8.1.1.6 Recording of both successful and failed system accesses.

8.1.1.7 Providing appropriate means for authentication; if a password management system is used, it should support quality passwords, (see Section 8.5.4, Password Management System).

8.1.1.8 Where appropriate, restrict the connection times of users.

8.1.1.9 Other access control methods, such as challenge-response, are available if these are justified on the basis of business risk.

8.1.1.10 Account lockout after three to five failed attempts to authenticate.

8.1.1.11 Do not display the last username used during logon.

8.1.1.12 Only authorized administrators shall have administrative access to the operating system. End users must be granted an exception for local administrative rights.

8.1.1.13 Each LegalMaps Information System must display an approved login banner/screen warning banner that identifies the system as the property of a corporation and is for "Authorized Use Only". In addition, it must make clear that the system is subject to monitoring, coupled with a requirement for the user's affirmative decision to accept the conditions in the banner notice by continuing to use the Information System. The following logon banner must be utilized:

WARNING! THIS SYSTEM IS FOR AUTHORIZED USE ONLY! The information on this computer and network is the property of a private corporation and is protected by intellectual property rights. You must be assigned an account on this computer to access information and are only allowed to access information as defined by the system administrators. Use of company resources should be for business purposes only and should be in compliance with the Code of Conduct and company policies and procedures. By accessing the property of a private corporation, your activities may be monitored and/or recorded and you should have no expectation of privacy on this computer and its networks. Use of this computer implies consent to monitoring and recording.

8.2 User Access Management

User Access management is required to enforce and maintain access control within the organization. Effective and consistent user access control will, in part, provide for proper access control throughout the organization.

The purpose of user access management is to prevent unauthorized access to business objects. User access controls should not reduce the productivity of users.

8.2.1 User Registration

Formal procedures for enrolling (setting-up for access) a user on a system must exist and should be followed in granting and revoking access to all business objects.

8.2.1.1 Every user must have a unique user ID and a personal confidential password or other trusted authentication method in order to gain access to LegalMaps' applications, databases, and network resources from a single authoritative source per Identity Management Technology. At its discretion, LegalMaps Security may require a secondary form of authentication, such as a token, before access to a system or service is granted. User IDs should not give any indication of the user's privilege level or role within LegalMaps.

8.2.1.2 User account names must use the LegalMaps Standard Naming convention.

8.2.1.3 Every request for a new or amended ID must be made on appropriate documentation and be validated by an Authorized business manager prior to being set up or amended.

8.2.1.4 Separate user IDs must be used to gain access to production and development environments such that full user accountability is maintained. A separate request must be made and authorized for each user ID.

8.2.1.5 Process or system IDs must be associated with a responsible and accountable user.

8.2.1.6 Users must construct passwords that conform to the LegalMaps Security standards as outlined in Section 8.3.1, *Passwords and PIN Use*.

8.2.1.7 In exceptional circumstances, where there is a clear business benefit, the use of a shared user ID for a group of users or a specific job can be used when approved by a Security Exception. Additional controls may be required to maintain accountability.

8.2.2 User De-Registration

When a user's access requirements change to warrant removal from a particular system (i.e. the user changes departments or job roles and should not have access to previous systems) or all systems (i.e. the user leaves LegalMaps), a user de-registration process must be carried out. The user's manager in conjunction with Human Resources and the security administrator is responsible for supporting the requirement that access rights are revoked or changed if the user changes job functions or leaves the organization.

8.2.3 Privilege Measurement

A privilege is any feature or facility of any system that enables a user to override system or application controls. The following are required as a part of user and system privilege management:

8.2.3.1 Privileged user access rights are to be reviewed at a more frequent interval; at least every 3 months and after any significant changes.

8.2.3.2 Authorizations for special privileged access rights are to be reviewed at more frequent interval; at least every 3 months.

8.2.3.3 Privileged allocations must be checked at regular intervals (at least every 3 months) to confirm that unauthorized privileges have not been obtained.

8.2.3.4 Systems and services (applications) accessing other systems should be subject to the same privileged management process as users. System privileges should be reviewed regularly (at least on a semi-annual basis, or after any changes to the access control rules of the underlying platform).

8.2.3.5 Systems and services that have special privileges should be reviewed more frequently (minimally on a quarterly basis, or after any changes to the access control rules of the business object).

8.2.3.6 Access control rules and business objects must be checked at regular intervals to confirm unauthorized privileges have not been obtained.

8.2.3.7 Creation, deletion, or change to a privileged user account must be logged.

8.2.3.8 If the creation, deletion, or change to a privileged user account cannot be logged, only a Director of LegalMaps may request a privileged user access change and only a Vice President (VP) or higher of LegalMaps may approve the request.

8.2.3.9 All privileged user change requests will be recorded and retained for two (2) years.

8.2.4 User Password Management

The allocation of passwords should be controlled through a formal management process. The Password Management System is out-lined in detail in Section 8.5.4, *Password Management System*.

8.2.5 Review of User Access Rights

To maintain effective control over access to data and information services, management should conduct a formal process at regular intervals to review users' access rights.

8.2.5.1 Users' access rights are reviewed at regular intervals (a period of every three (3) months is required at a minimum) and after any significant changes.

8.2.5.2 All user ID's shall have the associated privileges suspended after sixty (60) days of non-use and the user ID deleted after one hundred and twenty (120) days of non-use. Authorized user extended leave beyond thirty (30) days requires that the account be disabled and not set for deletion.

8.2.5.3 Managers must promptly notify their Security Administrator when users change departments or job duties in order to reduce system access rights that are no longer needed to perform their job. For job transfers, the user's prior supervisor is responsible for initiating the appropriate account deletion or access removal.

8.2.5.4 Managers must promptly notify their Security Administrator if a user will be on leave from work for more than thirty (30) days so that system access rights may be disabled.

8.2.5.5 Access control rules and business objects must be checked at regular intervals to validate that unauthorized user access has not been obtained.

8.3 User Responsibilities

Users should be made aware of their responsibilities for the passwords associated with their accounts, effective access controls they own and the security of user equipment. Procedures must be used such that only the password owner and the Information System the user uses/operates knows the password. Such awareness shall be provided by the required Security Awareness training.

8.3.1 Password and PIN Use

Controlling access to LegalMaps systems is essential; both to protect LegalMaps' information resources and to protect personal privacy. This need becomes increasingly vital as the systems are entrusted with more sensitive and valuable information. **All users and Information Systems must adhere to LegalMaps standard for password composition, change, and password uniqueness.**

8.3.2 Strong Authentication

Strong authentication requires approval from the LegalMaps Security Department within each scenario that requires strong authentication. It is usually denoted by factors greater than only username and password authentication and includes two-factor, biometrics and items of personal ownership such as digital keys. The definition of strong authentication is reliant on variable factors of the connection, user, and Information System that must be independently analyzed by LegalMaps Security prior to use.

Definition of Two-Factor Authentication

Two-Factor Authentication requires a primary factor, usually a username and password, combined with a unique secondary factor that must be related to "what you know" (username and password), "what you have" (SecureID token, certificate), or "what you are" (biometrics).

Strong Authentication for Dynamic Third Party Connections

Third party connectivity is often dynamic, for brief time periods, and usually for the purpose of remote problem diagnosis or training by an authorized vendor. The use of remote desktop services, (see Section 8.4.3 , *Remote Desktop Services*) is a common requirement. The following remote access policy applies to such connection types, although two-factor authentication must be redefined as follows:

Two-Factor Authentication for dynamic third party connectivity to remote desktop services, (e.g. WebEx or Terminal Services for remote training or diagnostics) may be provided by a temporary, unique username and password combined with a LegalMaps user that must authorize access, by means of manually accepting the remote connection and must monitor all access for the duration of connectivity. User presence with manual user authorization qualifies as an approved form of two-factor/strong authentication.

8.3.3 Tokens

If a user is supplied with a token as part of a two-factor authentication, that token must be unique to a single user. Unique data to that user must be embedded in the token and used by the authenticating server/system.

8.3.3.1 Tokens must be carried separately from the device used to access LegalMaps information. If a token is lost or stolen, it must be immediately reported to the Help Desk.

8.3.3.2 Tokens must not be shared or given to anyone other than the authorized user. To do so exposes the authorized user to responsibility for actions that the other party takes with the token. Similarly, users must not perform any activity with tokens belonging to others. Users are responsible for all activity performed with their token.

8.3.4 Group Account/Password Prohibition

A group account/password is a password or a User ID and password that is shared among a group of more than one user. LegalMaps prohibits the use of group accounts and associated passwords without an approved Security Exception. This Exception has to be fully documented outlining all security and mitigating controls around this user ID and password.

Group account and associated passwords assigned to system process or under third party agreements are allowed as necessary via an Exception, but their use is highly discouraged and must follow all other guidelines for usage.

8.3.4.1 Shared passwords must be encrypted when stored in files and databases.

8.3.5 Unattended User Equipment

Users should confirm that unattended equipment has appropriate protection to secure the equipment from unauthorized access or theft. All computer hardware and other necessary business equipment must be properly secured at all times, whether at an LegalMaps facility or alternative site such as home, hotel, or client site. Appropriate steps and due care must be taken to secure equipment against theft or damage. The steps users should take include, but are not limited to:

- Securing laptops and other equipment to user's desk using a cable and padlock
- Confirming that any equipment left in your vehicle is not visible. Equipment should be locked in the trunk of a user's vehicle. If a trunk is not available, LegalMaps equipment should be kept with the user at all times.
- Sensitive information, when printed, shall be cleared from printers immediately.

8.3.6 Clear Desk and Clear Screen Policy

All users must leave their desk/workstation clear of paper, disks, and storage media of any nature which may compromise the privacy and confidentiality of LegalMaps data and information. At the end of each working day, users must confirm at a minimum their PC/Terminal is logged off.

8.3.6.1 Screen Savers and Workstation Lockout

Screen saver software must be implemented that automatically locks or disconnects a workstation (includes terminals and PCs) session when inactivity thresholds are exceeded.

The maximum specified period of user inactivity must not exceed ten (10) minutes.

- The specified periods of time shall decrease as the level of sensitivity of the system accessed increases. Removal of this capability will require an approved Security Exception
- Unlocking the display screen must require the user to enter a unique password.

8.3.6.2 Unattended Workstation Lockout

Users must lock their workstations when left unattended to prevent unauthorized use.

8.4 Network Access Control

LegalMaps has an operational requirement to provide and manage access to LegalMaps information over all communications paths, both public and corporate. Electronically transmitted information is also considered a corporate asset and must be protected according to its classification level.

8.4.1 Policy on Use of Network Services

Users should only be provided with access to the services or applications that they have been specifically authorized to use.

8.4.1.1 Access rights to information must be assigned according to a user's job responsibilities and based on a "need to know". Managers are responsible for authorizing access to only the computer systems, files, or resources needed by users to perform their job duties.

8.4.1.2 Managers must consider separation of duties when authorizing system access rights for their users. No individual should be assigned a combination of duties or authorities that would be sufficient to subvert a business process which could be detrimental to LegalMaps.

8.4.1.3 Consultants, contractors, and temporary personnel are required to sign a system use/confidentiality agreement before accessing any of LegalMaps' resources.

8.4.1.4 Where possible, system access for consultants and temporary personnel must be created with an expiration date of six (6) months maximum or to coincide with the current contract term, whichever is shorter. A new request authorized by the user's supervisor is required to extend access.

8.4.2 User Authentication for External Connections (Remote Access)

External connections provide a potential for unauthorized access to business information, e.g. access by dial-up or direct-connect methods. Therefore, access by remote users is subject to strict rules of authentication and accountability.

Authentication of remote users must be achieved using methods of Strong Authentication as defined in Section 8.3.2, *Strong Authentication*, for example, a cryptographic based technique, hardware tokens, or a challenge/response protocol. Dedicated private lines or a network user address checking facility can also be used to provide assurance of the source of connections. Strong authentication by means of acceptable two factors of authentication is required for all dynamic and/or user based remote access.

External connectivity to the LegalMaps Information Systems, whether as a user or trusted partner, must adhere to the following requirements:

8.4.2.1 LegalMaps Security must approve any implementations of a Remote Access device or service before production operations.

8.4.2.2 All remote-access devices that provide authentication services shall be set to automatically logout a user account after eight (8) hours of inactivity.

8.4.2.3 All external access to corporate Information Systems via public networks, (i.e., Internet or shared communications medium) must be encrypted, employing the minimum levels of encryption as specified in Section 7.13, *Encryption Requirements*.

8.4.2.4 Devices that are capable of simultaneous remote access connections to both the LegalMaps network and any external network must be configured to meet LegalMaps standards for network security, including automatic disablement of split tunneling.

8.4.2.5 User remote access must be conducted via an approved method.

8.4.2.6 User remote access authentication must utilize strong authentication mechanisms approved by LegalMaps Security. (e.g. SecureID, biometrics, certificate, etc.).

8.4.2.7 Third parties must adhere to stipulations set forth in the LegalMaps Security Policy, contractual obligations and as specified in Section 7.2, *Third Party Service Delivery Management*, for all types of connectivity to Corporate Information Systems.

8.4.2.8 Third party connections must be assigned unique connection identifiers, authentication parameters, and implement firewall protection.

8.4.2.9 Temporary and/or infrequent third-party connections (dynamic) must adhere to the same rules of connectivity applied to users for remote access.

8.4.2.10 Modems should only be used for static trusted and contracted third party connections and must follow all policies for remote access, external connectivity, access control, authentication, accounting, and passwords.

8.4.2.11 Network attached devices that require or contain modems are permitted only if specifically approved and secured in accordance with LegalMaps security policies and with an approved Security Policy Exception.

8.4.2.12 All devices that provide remote access connectivity, and/or are capable of mobile usage, shall provide user identification, authentication, and audit logging in accordance with LegalMaps standards.

8.4.2.13 Audit logs on devices that allow remote-access connectivity and/or mobile usage shall be reviewed at a minimum on a monthly basis.

8.4.2.14 Access controls must be used to control remote users' access to information and resources on the LegalMaps network.

8.4.2.15 Remote access to Information Systems storing or processing PCI-defined cardholder information must utilize two-factor authentication.

8.4.2.16 The implementation of any hardware or software that facilitates or initiates remote access connections to the LegalMaps network shall be controlled and monitored under the following minimum requirements: User identification and authentication, Audit trail, Access control, and Cryptography.

8.4.2.17 The remote access device's operating system journal or log shall be used to monitor all communications activity with the host to determine system and network usage and uncover intrusions.

8.4.3 Remote Desktop Services

Remote Desktop Services are categorized as applications that provide administration or application usage by means of software capable of providing a graphical user interface to a user not local to the Information System or device. Examples of remote desktop services include, but are not limited to, Citrix Metaframe, GoToMyPC, WebEx, Microsoft Terminal Services, PCAnywhere, etc. The following controls must be adhered to for remote desktop services:

8.4.3.1 The user's supervisor prior to access must authorize all user use of remote desktop services. Type of access, (i.e. teleworking, emergency administration, etc.), services used (examples listed above), and intended access times must be defined within the access request form specifying remote desktop services.

8.4.3.2 Remote desktop hosting Information Systems, by default, fall under a Confidential classification (Class 3) and must be protected in accordance with all policies relating to such classification.

8.4.3.3 Localized, remote administration of Information Systems via remote desktop services by authorized LegalMaps system administrators must adhere to all policies set forth herein, specifically access control, authorization, accounting, strong authentication and password policies.

8.4.3.4 Remote Desktop services may be employed for temporary third party access, i.e. a vendor needs to view or manipulate a desktop for remote training or problem diagnosis. All such connections must adhere to the policies for dynamic remote access by a third party and must also have a valid third party agreement and non-disclosure agreement on file prior to access.

8.4.3.5 Authentication of the session and the session itself must meet all encryption requirements as defined Section 7.13, *Encryption Requirements*.

8.4.4 Equipment Identification in Networks

Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment when HIGHLY RESTRICTIVE resources or information is accessed.

Equipment identification can be used if it is deemed important by LegalMaps Security that the communications can only be initiated from a specific location or equipment to a particular resource or information. An identifier in or attached to the equipment may be used to indicate whether this equipment is permitted to connect to the restricted resource or information.

8.4.5 Remote Diagnostic and Configuration Protection

Physical and logical access to diagnostic and configuration of system components should be controlled. Any connection from outside the protected network used to access an LegalMaps system for maintenance or configuration shall be protected by physical and procedural controls, including training of authorized users, restricting use to authorized users, and maintenance of a usage access log. In addition:

8.4.6.1 Only a limited number of LegalMaps users shall have remote diagnostic access. These users must be properly identified and have appropriate clearances.

8.4.6.2 Unique User IDs must be used for each user. Users should be instructed that they must never share their ID or password.

8.4.6.3 Access should be limited by source, destination, and protocol where applicable.

8.4.6.4 When a vendor must have remote maintenance access for system maintenance, means shall be provided to properly identify, authenticate, and audit such access sufficiently enough to provide assurance at least equivalent to the former controlled access protection level. This may be achieved by procedural controls such as manual enabling and disabling remote access for the period of required access or use of approved remote access methods, such as secure virtual private networks.

8.4.6 Segregation in Networks

Groups of information services, users, and Information Systems should be segregated on networks. The introduction of controls within the network is required to segregate groups of information services, users, and Information Systems. Networks should be segmented by a combination of the following as a minimum: Gateways and Firewalls (See Section 8.4.9 below), Virtual Local Area Networks (VLANS), Network address segmentation and routing controls, and private addressing, (RFC 1918).

8.4.7.1 Networks are to be segregated by function. For example, the corporate network should be segregated from Production, Development, and Internet facing networks. The Production network should be segregated from the Development and all other networks. Internet facing networks should be segregated from any internal LegalMaps networks. Database servers should be separated from presentation and application servers.

8.4.7 Network Connection Control

For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network should be restricted, in line with the access control policy and requirements of the business applications.

8.4.8 Network Routing Control (Gateways/Firewalls)

Shared networks, especially those extending across organizational boundaries, require the incorporation of routing controls such that computer connections and information flows do not breach the access control policy of the business applications.

Routing controls should be based on positive source and destination address checking mechanisms. Network address translation is also a very useful mechanism for isolating networks and preventing routes to propagate from the network of one organization into the network of another. They can be implemented in software or hardware. All LegalMaps information networks must be segmented by network traffic filtering devices from public networks, private networks, and third-party connections. The following controls have been established to provide a baseline for secure network connectivity:

8.4.9.1 All connections to the Internet must be protected, at minimum, by stateful inspection network layer firewalls that employ both extensive audit trails and real-time alarms. Certified firewall products that have passed professional evaluations such as Common Criteria 2.1 are advised.

8.4.9.2 All trusted third-party connections must have network access filtered and monitored by at least one firewall with appropriate audit trail capabilities.

8.4.9.3 Wide area connectivity between geographically separated business units, subsidiaries, or operating partners, or any other trusted corporate entity must be protected, at minimum, by stateful inspection network layer firewalls that employ both extensive audit trails and real-time alarms. Certified firewall products that have passed professional evaluations such as Common Criteria are advised.

8.4.9.4 All firewalls must employ address spoofing controls and malicious activity deterrence for, at a minimum, Distributed/Denial of Service (D/DOS) attacks.

8.4.9.5 Policies of default deny must be employed by all gateways/firewalls for both incoming and outgoing rules for all attached networks. No information shall pass through a gateway/firewall unless authorized by rules specific to, at a minimum, the network protocol to be utilized.

8.4.9.6 Application layer inspection of protocols considered critical to the protected environment must be employed via Intrusion Prevention Systems (IPS) / Intrusion Detection Systems (IDS).

8.4.9.7 Prohibiting an external network direct public access to any system component that is storing bank account, routing, credit card holder data, and personally identifiable information.

8.4.9.8 Implementation of Internet Protocol (IP) masquerading to prevent internal addresses from being translated and revealed on public networks. Use technologies such as Port Address Translation (PAT) or Network Address Translation (NAT).

8.4.9 Application Layer Inspection Requirements

Connections utilizing encryption such as SSL should demark at the perimeter firewalls such that information may be scanned by firewalls, intrusion detection/prevention systems, and any other application layer inspection device or service, or have a Host Based IPS/IDS deployed on the web server.

Firewalls, intrusion monitoring, and network inspection devices must be capable of application layer inspection of all protocols utilized for public communications of public Information Systems (e.g. HTTP, FTP and SMTP must be inspected up to the application layer by such devices such that the content of the message is inspected for potentially malicious content and errors.)

8.4.10 Tiered Security Infrastructure Design Requirements

Systems that process or store information deemed LegalMaps-Confidential (Class 3) or LegalMaps-Restricted (Class 4) must have all such sensitive information placed behind, at a minimum, a second layer firewall protecting direct access to sensitive information. Equally, those systems that process or store critical information are required to place front-end applications that access the sensitive information behind a single, first layer firewall. An example of such a configuration would be a Web user interface placed behind a single firewall and the database containing critical information behind a second firewall within a secured region.

8.4.11.1 Deviations from use of gateway/firewall require a dedicated hardware device with configuration to prohibit any Transport Control Protocol (TCP) or User Datagram Protocol (UDP) service that is not explicitly permitted along with approved operating system hardening as defined in Section 8.5 below, *Operating System Access Control* and approval by LegalMaps Security with an accompanying risk assessment and a product assurance review of the proposed alternative.

8.5 Operating System Access Control

The LegalMaps operating system access controls are a compilation of security configuration actions and settings that "harden" operating systems. These procedures describe practices that counter common, known attacks on network installations that expose or modify user data maliciously. The goal is to make these platforms as secure as can *reasonably and practically* be configured. Some controls may impede operational capability; therefore, their use must be carefully balanced against the security they offer. The following apply to hardening requirements for LegalMaps Information Systems:

a. All server-based Information Systems must be hardened to LegalMaps standards for hardening of each operating system.
b. LegalMaps Security Assessments in coordination with the assigned security administrator must validate that LegalMaps hardening procedures are enforced on all server-based Information Systems.
c. The hardening procedures should be reviewed annually and kept up to date as new vulnerabilities are discovered.
d. If available, hardening requirements shall be based on recommended best practices published by the operating system vendor, CIS Standards, the National Security Agency (NSA)/National Institute of Standards and Technology (NIST).

Teams including LegalMaps Security, IT Governance, and IT are responsible for reviewing, modifying, testing, and distributing all LegalMaps platform-hardening procedures. When conditions warrant an update to existing procedures, these following actions will be performed:

a. Update the appropriate procedure(s);
b. Perform a new build of the operating system based upon the modified procedures;
c. Perform comprehensive controlled penetration testing against the platform;

Multifunction devices, (i.e., printer/fax/copier) employing local area network connectivity must be hardened prior to deployment such that default passwords have been changed to meet policy requirements and all remote management services, specifically Web and SNMP management, be disabled unless absolutely required.

8.5.1 Application and Operating System Version Control

All commercial applications running on Public or Corporate Information Systems (Class 3) or above must not be behind more than one major code release for all software and operating systems. If a new vulnerability has been publicly announced that could be mitigated by the application of a new code revision or patch, it must be applied as soon as possible, and after testing in a non-production environment to avoid security compromise on suspected systems. If the new code release cannot be implemented, it must be documented and brought forth to the Director of Information Security for approval.

8.5.2 Secure Log-on Procedures

Access to operating systems should be controlled by a secure log-on procedure.

8.5.2.1 Passwords or PINs should not pass in clear text to the authenticating system.

8.5.2.2 Passwords should be stored encrypted.

8.5.3 User Identification and Authentication

All users should have a unique identifier (user ID) for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of the user. The creation or a reset of a user's ID password should be unique or randomly generated. More details on user identification and authentication may be found in Section 8.2, *User Access Management*.

8.5.4 Password Management System

The allocation of passwords should be controlled through a formal management process to validate that the security, integrity, confidentiality, and accountability of LegalMaps systems and information.

An approved password management system shall:

8.5.4.1 Enforce the use of individual passwords to maintain accountability.

8.5.4.2 Where appropriate, allow users to select and change their own passwords and include a confirmation procedure to allow for input errors. Password change procedures must verify the identity of a user requesting a password change prior to allowing the password to be changed.

8.5.4.3 Enforce passwords that meet or exceed LegalMaps policy requirements.

8.5.5 Use of System Utilities

Most computer installations have one or more system utility programs that might be capable of overriding system and application controls. It is essential that their use is restricted and tightly controlled.

8.5.5.1 Use of authentication procedures for system utilities.

8.5.5.2 Segregation of system utilities from applications software.

8.5.5.3 Limitation of the use of system utilities to the minimum practical number of authorized users.

8.5.5.4 Authorization for ad hoc use of systems utilities.

8.5.5.5 Limitation of the availability of system utilities, e.g. for the duration of an authorized change.

8.5.5.6 Logging of all use of system utilities.

8.5.5.7 Defining and documenting authorization levels for system utilities.

8.5.5.8 Removal or disablement of all unnecessary software based utilities in accordance with system hardening procedures.

8.5.6 Limitation of Connection Time

Restrictions on connection times should provide additional security for high-risk applications. Limiting the period during which terminal connections are allowed to computer services reduces the window of opportunity for unauthorized access. Such controls are required for sensitive computer applications, especially those with terminals installed in high-risk locations, e.g. public or external areas that are outside the organization's security management. Examples of such restrictions include:

a. Using predetermined time slots, e.g. for batch file transmissions, or regular interactive sessions of short duration;

b. Restricting connection times to normal office hours if there is no requirement for overtime or extended-hours operation.

8.6 Application Access Control

Security facilities should be used to restrict access within application systems. Logical access to software and information should be restricted to only prior authorized users. Application systems must:

a. Control user access to information and application system functions, in accordance with a defined business access control policy;
b. Provide protection from unauthorized access for any utility and operating system software that is capable of overriding system or application controls;
c. Not compromise the security of other systems with which information resources are shared;
d. Be able to provide access to information to the owner only, other nominated authorized individuals, or defined groups of users.
e. The Information System privileges of all systems and programs shall be limited to the access required to meet the business needs.
f. Where possible user access should not be granted directly to the resources. User access should be restricted to the application and the application granted access to the resources.

8.6.1 Information Access Restriction

Users of application systems, including support staff, should be provided with access to information and application system functions in accordance with a defined access control policy, based on individual business application requirements and consistent with organizational information access policy. Application of the following controls is required in order to support access restriction requirements:

8.6.1.1 Provide menus to control access to application system functions.

8.6.1.2 Control the access rights of users, e.g. read, write, delete and execute.

8.6.1.3 Confirm that outputs from application systems handling sensitive information contain only the information that is relevant to the use of the output and are sent only to authorized terminals and locations.

8.6.2 Sensitive Information System Separation

Sensitive systems require a dedicated (isolated) computing environment. A sensitive system is any system classified as LegalMaps-Confidential (Class 3) or LegalMaps-Restricted (Class 4), and/or has public exposure. The sensitivity and associated risks may indicate that the application system should be physically or logically separated and should only share resources with trusted applications systems.

The use of firewalls and/or network segmentation with Access Control Lists (ACLs) should be used so that sensitive systems do not reside on the same subnet or network segment as other Information Systems of lower classification. Each Information System must be defined by an owner and given a classification as a part of the Risk Assessment process. Differing Information Systems may communicate as deemed necessary but must use authorized communication channels that are adequately protected by restriction of protocols, access controls and authorization as defined by the requirements for access controls, gateways and firewalls.

Firewalls must be utilized throughout the organization where connectivity to external networks has been provided. Firewalls must also be used to separate sensitive information from the applications utilizing such

information and from other corporate and public Information Systems as defined by segmentation requirements. The following requirements apply:

8.6.2.1 The sensitivity of an application system should be explicitly identified and documented by the Information System owner.

8.6.2.2 When a sensitive application is to run in a shared environment, the applications with which it will share resources should be identified and agreed with the owner of the sensitive application.

8.6.2.3 Public exposure and exposure to other geographically separated business units must be taken into account when considering segmentation and network security of sensitive systems.

8.6.2.4 Sensitive information must be physically or logically separate from the application(s) that process such information. Separation must be in the form of network segmentation, physical segmentation, or network firewalls to separate the systems into a minimum of two processing tiers.

8.6.2.5 Sensitive systems should be restricted to only one application or primary function per server.

8.7 Mobile Computing and Teleworking

The term “mobile systems” means any corporate information device that is in use and not in a fixed location (most commonly laptops, but it also includes PDA’s, cell phones, etc.). Throughout this policy, mobile systems may be quantified as “devices capable of mobile processing and storage of digital information”, i.e. any device that is not fixed in its location and can leave a LegalMaps physical environment.

8.7.1 Protection Measures for Mobile Computing Devices

8.7.1.1 Hard drive encryption software must be installed, configured, and properly running on laptop computers.

8.7.1.2 Software firewalls capable of stateful inspection must be employed on all laptop computers, when the capability exists. The ability to disable such software shall not be allowed.

8.7.1.3 Virus scanning software must be employed by all laptop computers and should be setup to automatically update virus definitions at a minimum every 24 hours, when the capability exists.

8.7.1.4 All use of remote control software on any modem-connected or VPN-connected device, which is also attached to the LegalMaps network must be approved before implementation and meet all policies for remote desktop services as defined in Section 8.4.3 *Remote Desktop Services*.

8.7.2 Responsibility for Mobile Computing Devices

LegalMaps users are responsible for the end security of mobile computing devices. LegalMaps Security mandates mobile computing device security and Technology Operations is responsible for confirming that new releases of the standard security configuration are propagated onto all mobile computing devices under their control in a timely manner. In addition, the Technology Operations group is responsible for communicating with staff to confirm security requirements are satisfied.

8.7.3 Responsibility for Security Configuration

LegalMaps Security is responsible for establishing and maintaining the standard security configuration of mobile computing devices under their control. Additional responsibilities include the testing of new software releases, training staff, and coordinating policies related to mobile computing and remote access. Further, reporting of incidents must be in accordance with Section 10.1, *Reporting Security Events*. LegalMaps

Security should evaluate the efficacy of the security controls at least annually or when an issue of configuration or deployment creates a substantial risk to LegalMaps.

8.7.4 Use of Privately Owned Mobile Computing Devices

Privately owned computers or mobile computing devices are prohibited from accessing LegalMaps networks or storing sensitive LegalMaps information.

8.7.5 Centralized Monitoring for Mobile Computing Devices

All mobile computing devices that participate in remote access to LegalMaps networks and Information Systems must be monitored and controlled so that any changes in the status of their security is detected and managed. Non-compliance with the requirements for portable electronic devices should be detected, and remote access disallowed until compliance has been met.

9 Information Systems Acquisition, Development and Maintenance

The security objectives within systems acquisition, development and maintenance are to support the requirement that security is built into Information Systems applications and processes are developed and followed that provide for a controlled systems development life-cycle methodology (including, but not limited to, infrastructure such as voice and data networks, business applications such as software developed for e-commerce or for sale to a customer, and user-developed applications).

The design and implementation of the business process supporting the application or service can be critical for security. Security requirements must be identified, reviewed, and agreed upon.

9.1 Security Requirements Analysis and Specifications

Security control requirements should be specified during the requirements' phase of new Information Systems and be included in the initial planning stages for enhancements to existing systems. Equally, maintenance of Information Systems must also adhere to the same standards to provide for the consistent delivery and operation of secure Information Systems. The following policies outline requirements and recommendations as they pertain to secure development and maintenance of LegalMaps Information Systems and applications.

Security requirements and controls should reflect the business value of the resources involved, the sensitivity of the data, legal and regulatory requirements, and the potential business damage, which might result from a failure or absence of security.

The framework for analyzing security requirements and identifying controls to fulfill them is through a risk assessment integrated into the LegalMaps PMO Process.

9.2 Correct Processing of Data in Applications

Appropriate controls and audit trails or activity logs should be designed into all applications. These should include the validation of input data, internal processing and output data.

Additional controls may be required for systems that process, or have an impact on, sensitive, valuable or critical organizational assets. Such controls should be determined on the basis of security requirements and risk assessment that can then be correlated with data classification with subsequent requirements outlined within associated protection matrices located in Section 4, *Asset Management*.

Managers responsible for application development and Information Systems are responsible for the security of the project or supported environment. They should validate that all proposed system changes are reviewed to check that they do not compromise the security of either the application or the operating environment.

9.2.1 Input Data Validation

Data input to application systems should be validated to confirm that it is correct and appropriate. Checks should be applied to the input of business transactions, standing data (names, addresses, social security numbers…) and parameter table (sales prices, rates…). All software shall verify and acknowledge user input, regardless of outcome. Data sanitation controls should be applied to prevent vulnerabilities such as buffer overflows and SQL Injection.

9.2.2 Control of Internal Processing

Validation checking should be integrated into applications to detect bad data resulting from incorrect processing or deliberate misuse.

The following controls are required, at a minimum, when developing applications requesting user input:

9.2.2.1 Dual input or other input checks to detect the following errors:

- Out-of-range values
- Invalid characters in data fields
- Missing or incomplete data
- Exceeding upper and lower data volume limits, Unauthorized or inconsistent control data.

9.2.2.2 Periodic review of the content of key fields or data files to confirm their validity and integrity:

- Inspecting hard-copy input documents for any unauthorized changes to input data (all changes to input documents should be authorized)
- Procedures for responding to validation errors
- Procedures for testing the plausibility of the input data
- Defining the responsibilities of all personnel involved in the data input process.

9.2.3 Areas of Risk

Data that has been correctly entered can be corrupted by processing errors or through deliberate acts. Validation checks should be incorporated into systems to detect such corruption. The design of applications should confirm that restrictions are implemented to minimize the risk of processing failures leading to a loss of integrity. Specific areas to consider include:

- The use and location in programs of add and delete functions to implement changes to data;
- The procedures to prevent programs running in the wrong order or running after failure of prior processing (see also Section 7.1.1, *Documented Operating Procedures*);
- The use of programs to recover from failures to provide for the correct processing of data.

9.2.3.1 Checks and Controls

The controls required will depend on the nature of the application, the classification of data, and the business impact of any corruption, theft or loss of data. Examples of checks and controls that must be incorporated include the following:

- Session or batch controls, to reconcile data file balances after transaction updates;
- Balancing controls, to check opening balances against previous closing balances, namely:
  - Run-to-run controls;
  - File update totals;
  - Program-to-program controls;
  - Validation of system-generated data;
  - Checks on the integrity of data or software downloaded, or uploaded, between central and remote computers;
  - Hash totals of records and files;
  - Checks to confirm that application programs are run at the correct time; and
  - Checks to confirm that programs are run in the correct order and terminate in case of a failure, and that further processing is halted until the problem is resolved.

9.2.4 Message Integrity

Message integrity is a technique used to detect unauthorized changes to, or corruption of, the contents of a transmitted electronic message. It can be implemented in hardware or software supporting a physical message authentication/integrity device or a software algorithm.

Message integrity is required for applications where there is a security requirement to protect the integrity of the message content, e.g. electronic funds transfer, specifications, contracts, proposals etc with high importance or other similar electronic data exchanges.

Message integrity is not designed to protect the contents of a message from unauthorized disclosure. Cryptographic techniques (see Section 9.3, *Cryptographic Controls*) can be used as an appropriate means of implementing message integrity.

9.2.5 Output Data Validation

Data output from an application system must be validated such that the processing of stored information is correct and appropriate to the circumstances. Typically, systems are constructed on the premise that having undertaken appropriate validation, verification and testing the output will always be correct. This is not always the case. Output validation requirements are as follows:

- Plausibility checks to test whether the output data is reasonable;
- Reconciliation control counts to provide for processing of all data;
- Providing sufficient information for a reader or subsequent processing system to determine the accuracy, completeness, precision and classification of the information;
- Procedures for responding to output validation tests;
- Defining the responsibilities of all personnel involved in the data output process.
- Proper output encoding controls to prevent vulnerabilities such as Cross-Site Scripting (XSS).
- Checks to confirm the error events do not expose verbose error messages that can lead to compromise of application and data confidentiality.

9.3 Cryptographic Controls

LegalMaps programs using cryptography are required to use the management schemes as defined by this policy document. The use of cryptography will be determined by the data classification on the system in question.

9.3.1 Policy on the Use of Cryptographic Controls

Making a decision as to whether a cryptographic solution is appropriate should be seen as part of a wider process of assessing risks and selecting controls. A risk assessment and data classification should be carried out to determine the level of protection that information should be given. This assessment can then be used to determine whether a cryptographic control is appropriate, what type of control should be applied and for what purpose and business processes.

9.3.2.1 Required Policy and Practices Documentation

The Information Security Owner or Manager for each business unit is responsible for obtaining approval of their use and practices document of digital signatures (i.e. *Certificate Policy, Certificate Practices Statement*). Guidelines for establishing policy and practices documents are provided in American National Standards Institute (ANSI) X9.79, *Public Key Infrastructure Practices and Policy Framework*. Security Engineering must authorize any changes to an operational system using digital signatures if such changes result in modifications to either the policy or practices documents.

9.3.2 Non-Repudiation Services

In general terms, the term "non-repudiation" crypto-technically means:

- In authentication, a service that provides proof of the integrity and origin of data, both in an unforgeable relationship, which can be verified by any third party at any time; or,
- In authentication, an authentication that with high assurance can be asserted to be genuine, and that cannot subsequently be refuted.

Non-repudiation services should be used where it might be necessary to resolve disputes about occurrence or non-occurrence of an event or action, e.g. a dispute involving the use of a digital signature on an electronic contract or payment. They can help establish evidence to substantiate whether a particular event or action has taken place, e.g. denial of sending a digitally signed instruction using electronic mail. These services are based on the use of encryption and digital signature techniques.

9.3.3 Key Management

Key Management is the secure administration, implementation and use of cryptographic keys throughout their Life Cycle, which includes its generation, distribution/receipt, loading/entry, storage and archival, destruction and for some asymmetric keys, registration. Sound key management practices protect cryptographic keys from disclosure, substitution, replacement or misuse and thereby reducing the threat to cryptographic applications and decreasing business risk.

The Key Life Cycle is the same for an asymmetric private key as it is for a symmetric key, unless otherwise specified. The Key Life Cycle differs for an asymmetric public key after the key generation step.

The contents of service level agreements or contracts with external suppliers of cryptographic services, e.g. with a certification authority, should cover issues of liability, reliability of services and response times for the provision of services (see Section 7.12, *Outsourcing*).

The following are requirements under key management:

9.3.4.1 Key management processes and procedures shall be sufficiently documented to enable all personnel to consistently apply the procedures, and enable the reconstruction of all related activities.

9.3.4.2 Dual control shall be used for all key components.

9.3.4.3 Cryptographic keys, when in multiple component or share form, shall be entrusted to and controlled by two or more key custodians.

9.3.4.4 One key custodian shall not have access to, or knowledge of, all key components or share values.

9.3.4.5 Physical access to cryptographic materials and equipment shall be limited to authorized individuals.

9.3.4.6 No more than two entities shall use a symmetric key and no more than one entity shall use an asymmetric private key.

9.3.4.7 A key used in a production system or environment shall not be used in a test or non-production system or environment.

9.3.4.8 Keys shall only exist in one of the following forms: As a clear key in a Tamper Resistant Security Module (TRSM), As two or more components or shares using dual control and split knowledge, or Encrypted by another key of equal or greater length.

9.3.4 Cryptographic Strength

9.3.5.1 Keys shall be replaced prior to the time feasibly required to determine them through crypto-analysis, i.e. a dictionary attack.

9.3.5.2 A key shall not be used to provide for the security or integrity of data where it is feasible to determine that key in a period of time less than the useful life of that data.

9.3.5 Key Generation

In order to reduce the likelihood of compromise, keys should have defined activation and deactivation dates so they can only be used for a limited period of time. This period of time should be dependent on the circumstances under which the cryptographic control is being used and the perceived risk.

In addition, the following apply:

9.3.6.1 Keys or components shall be generated using a random or pseudo-random process.

9.3.6.2 A resulting asymmetric key shall be equally segmented.

9.3.6.3 The length of each component of a symmetric key shall be equivalent to the length of the resulting key.

9.3.6 Key Storage

Keys and their components or shares shall exist in the fewest possible locations and forms necessary to enable their effective use. Systems utilizing keys shall prevent the disclosure of any key that has been used to encipher any still-secret or confidential data with the exception of asymmetric public keys.

9.3.7 Key Transport

All clear-text key components or shares shall be transported either in person or via a courier. Any other means for transporting clear-text key components or shares shall be approved in writing by LegalMaps Security. Both the sending and receiving entities shall each use two or more designated key custodians. When transporting clear-text key components or shares via a courier the following must be adhered to:

- Only secured couriers shall be used.
- The components or shares shall be enclosed in tamper evident packaging in addition to the courier packaging.
- The components or shares shall be sent either using different couriers or different days.
- When transporting clear-text key components or shares in person:
    1. Each designated Key Custodian shall retain physical possession of the component or share during transport.
    2. The components or shares shall be enclosed in either tamper evident packaging or an approved security container.

9.3.8 Key Usage

Each key shall be: Associated with a specific protocol or set of related protocols, Associated with only one key type, Unique, and Used for the sole purpose for which it is intended.

All systems utilizing keys shall be capable of determining a key's type and Identifying a key associated with more than one key type.

9.3.9 Key Destruction

All active instances of cryptographic keys shall be erased and destroyed at the end of the key's life cycle.

9.3.10 Key Compromise

Mechanisms shall exist to either prevent or confirm the detection of unauthorized attempts to disclose, access, use, modify or substitute a key or key component, or restore a key known or suspected of compromise.

The following requirements pertain to the protection and mitigation of key compromise:

9.3.11.1 All key management processes shall include a means for detecting the compromise or use of a key for unauthorized purposes.

9.3.11.2 A compromised key shall not provide any information used to determine its replacement.

9.3.11.3 A cryptographic key or component suspected, or known to be compromised shall be replaced. A suspected compromise includes, but is not limited to:

- A key or component of unknown authenticity, security, or integrity.
- A key used for more than its intended purpose.
- A key protected by a compromised key.

9.3.11 Audit Trails for Key Management

All key management activities shall be logged and maintained for all actions that occur within the life cycle of cryptographic key or key components. System related activities shall be logged in accordance with, Section 7.11.3 *Monitoring System Use*. Additionally, the following apply to audit trails for key management:

9.3.12.1 Audit trails shall be retained for a given key throughout the life and for three (3) years subsequent to the destruction and/or deletion of the key.

9.3.12.2 Audit trails shall identify, at a minimum, when the key activity occurred, why, by whom, the key(s) involved and any hardware involved.

9.3.12.3 Audit trails shall be secured such that only authorized persons can read them and they cannot be modified.

9.3.12.4 Audit trails shall be reviewed at least annually.

9.3.12 Key Custodian Requirements

9.3.13.1 A Key Manager shall designate key custodian responsibilities.

9.3.13.2 Key Custodian credentials shall be established and validated.

9.3.13.3 One key custodian shall not report to an individual that either is or has been a custodian of a different component or share of the same key. A custodian may report to another custodian, provided he or she, either is or has been the custodian of the same component or share, or of an unrelated key.

9.3.13.4 Each Key Custodian shall sign a Key Management nondisclosure agreement.

9.4 Security of System Files

Access to system files should be controlled through, at a minimum, discretionary access control methods and/or Role Based Access Controls, including strict file and directory permissions in accordance with operating system hardening procedures.

9.4.1 Control of Operational Software

Control should be provided for the implementation of software on operational systems. To minimize the risk of corruption of operational systems, the following controls are required:

9.4.1.1 The updating of the operational program libraries shall only be performed by the nominated librarian upon appropriate management authorization (see Section 9.4.3, *Access Control to Program Source Libraries*).

9.4.1.2 Operational systems should only hold executable code.

9.4.1.3 Development staff must not have the ability to independently move any software into the production environment.

9.4.1.4 Executable code shall not be implemented on an operational system until evidence of successful testing and user acceptance is obtained, and the program source libraries have been updated.

9.4.1.5 Prior to moving software into production, developers and other technical staff must remove all special access paths so that access may only be obtained via authorized security channels. This provision would include the removal of all back doors, short cuts, and special system privileges needed for development or testing that could be used to compromise the security of the production environment.

9.4.1.6 Software development staff must not be permitted to access production information unless it is relevant to the particular project for which they are currently working. Where access to production information is required for development, testing, or support purposes, only "read" and "copy" access may be granted.

9.4.1.7 An audit log shall be maintained of all updates to operational program libraries.

9.4.1.8 Previous versions of software shall be retained outside of the operating environment as a contingency measure.

9.4.1.9 Software in development or testing must be kept strictly separate from production software. If existing facilities permit, this separation must be achieved both physically and logically. When computing facilities do not allow this, separate directories or libraries with strictly enforced access controls must be employed.

9.4.1.10 System developers and technical staff are individually responsible for notifying management about any technical problems or security vulnerabilities which might be caused by the applications or systems they are building, installing, or modifying.

9.4.1.11 Vendor supplied software used in operational systems shall be maintained at a level supported by the supplier and in compliance with patch management policies see Section 9.6.1, *Patch Management*.

9.4.1.12 Physical or logical access should only be given to vendors for support purposes when necessary, and with security approval. The vendor's activities must be sufficiently monitored.

9.4.2 Protection of System Test Data

System and acceptance testing usually requires substantial volumes of test data that are as close as possible to production data. The following controls should be applied to protect operational data, when used for testing purposes.

9.4.2.1 All testing for systems designed to handle customer or LegalMaps sensitive information cannot use production information or databases unless it has been "sanitized" or approved for use in testing by Security

Investigations and Credentialing. Sanitized information is production information that no longer contains specific customer or LegalMaps sensitive details.

9.4.2.2 The access control procedures, which apply to production application systems, must also apply to test application systems.

9.4.2.3 There shall be separate authorization each time production data is copied to a test application system.

9.4.2.4 Production information shall be erased from a test application system immediately after the testing is complete.

9.4.2.5 The use of production information must be logged to provide an audit trail.

9.4.3 Access Control to Program Source Libraries

In order to reduce the potential for corruption of computer programs; strict control should be maintained over access to program source libraries as follows:

9.4.3.1 Program source libraries should not be held in operational systems.

9.4.3.2 A program librarian should be nominated for each application.

9.4.3.3 IT support staff should not have unrestricted access to program source libraries.

9.4.3.4 Operational program source libraries shall not be used for development or maintenance.

9.4.3.5 The updating of program source libraries and the issuing of program sources to programmers should only be performed by the nominated librarian upon authorization from the IT support manager for the application.

9.4.3.6 An audit log should be maintained of all accesses to program source libraries.

9.4.3.7 Old versions of source programs should be archived, with a clear indication of the precise dates and times when they were operational, together with all supporting software, job control, data definitions and procedures.

9.4.3.8 Maintenance and copying of program source libraries should be subject to strict change control procedures.

9.4.4 Control of Internal Processing

All applications shall check and verify boundaries of data transferred to and from blocks of memory to prevent overwriting of critical data and programs.

9.5 Security in Development and Support Processing

Security in development and support processing is the on-going process of identifying and resolving specific security vulnerabilities for a given Information System. All resources and assets, and the systems [networks, connections, etc.] on which they depend, are subject to the vulnerability management policy.

9.5.1 Covert Channels and Trojan Code

Any undesired exposure of information by some indirect and obscure means is a covert channel. It may be possible to trigger a covert channel by changing a parameter that makes information accessible to both insecure systems and secure systems.

Trojan Code is code that is designed to produce unauthorized access to a system or information, and is not easily noticed or detected.

All code review personnel and development managers should adhere to the following:

a. Purchase software from reputable vendors.
b. If possible, obtain software in source code, so a code reviewer may validate its functionality
c. Evaluate and test the function of all software before its use.
d. LegalMaps Security reserves the right to inspect and validate all source code before the software is put into operational or production environments.
e. Access to all source code must be protected in accordance with this policy to prevent unauthorized modification, theft, or loss.

9.5.2 Change Control Procedures

Change Control procedures are to be used to confirm changes to applications and systems are authorized, tested, recorded, and maintained for version control. As part of a change control process the following controls must be adhered to:

9.5.2.1 Developers shall not have access to production. With an approved Security Exception, developer access may be granted to read-only access to production systems.

9.5.2.3 Changes should never be made without proper versioning and authorization.

9.5.2.4 Changes to operational or production systems are to be done by authorized staff only.

9.5.2.5 All change requests and implementations shall be recorded in an audit trail.

Formal Change Control Procedures should be developed and followed for all development tasks. The procedures should include, at a minimum:

9.5.2.6 A process to confirm that changes are submitted by authorized users.

9.5.2.7 Change Authorization processes to confirm changes are approved.

9.5.2.8 A process to confirm all system documentation is updated in the event of a change.

9.5.2.9 A process to confirm that implementation of the change will minimize interruption of business activities, including the business activity involved with the change.

9.5.2.10 Changes need to consider the impact on the DR/BCP capabilities and the need to mirror them to the DR environment.

9.5.2.11 Changes that have an impact on the security of any service/process/system, should be highlighted and require LegalMaps Security signoff.

9.5.2.12 Any change to a system or process that falls under the Sarbanes Oxley (SOX) requirement, should be highlighted and require SOX process owner review signoff.

9.5.2.13 Change requests must include plans for testing and back-out procedures.

9.5.3 Technical Review of Operating System Changes

Periodically, it is necessary to change the operating system, e.g. to install a newly supplied software release or patches. When changes occur, the application systems must be immediately reviewed and tested to confirm that there is no adverse impact on operation or security.

9.5.4 Restrictions on Changes to Software Packages

Modifications to vendor software packages at a code level are prohibited. All required changes must be supplied by the vendor.

9.5.5 Information Leakage

Opportunities for information leakage or exploitation of covert channels should be prevented through the use of:

- Scanning of outbound media and communications for hidden information;
- Masking and modulating system and communications behavior to reduce the likelihood of a third party being able to deduce information from such behavior;
- Making use of systems and software that are considered to be of high integrity;
- Monitoring resource usage in computer systems.

9.5.6 Outsourced Software Development

If development activities are outsourced, done by a third-party, the following are required to comply with the LegalMaps Security Policy for Suppliers and LegalMaps Application Software Security Policy:

9.5.6.1 An agreement that clearly states the desired Licensing ownership, code ownership and Intellectual Property Rights is required with third-parties.

9.5.6.2 The right to audit the third-party must be clearly stated in the agreement with the third party.

9.5.6.3 A process to certify the quality and accuracy of the work done by the third-party, and a supporting agreement that requires quality of code based on the certification process.

9.5.6.4 The use of escrow arrangements in the event of third-party failure to deliver must be indicated in the third party agreement.

9.5.6.5 An internal code review team to test and review the code (also to check for Covert Channels and/or Trojan Code) must be used before code is put into production.

Additional requirements can be reviewed in detail in the above noted policies.

9.6 Technical Vulnerability Management

As a part of the security program, all sensitive Information Systems, new or modified, shall undergo a vulnerability assessment.

All vulnerabilities identified will be assessed for risk level, and the asset owner will coordinate resolutions for mitigating the risk prior to production activities. All exceptions to policy must be documented by means of a formal security policy exception request.

9.6.1 Control of Technical Vulnerabilities - Patch Management

Patch management is the process of consistently maintaining application and operating system software versions up to levels that may prevent exploitation of flaws in the software.

LegalMaps Security will monitor various vulnerability alert resources and may issue alerts as necessary. Patch management alerts should indicate the assessment rating of the vulnerability as defined by the reporting agency, (e.g. CERT, vendor, etc.) or LegalMaps Security and the schedule for applying the patch, as follows:

Patch Management Alert and Response Matrix		
Patch Assessment	**Impact Analysis**	**Application**
Critical Risk	• Major impact on systems performance or network availability or data integrity is occurring or exploit code is released publicly and threat is imminent.	Within 48 hours and as soon as practical following testing, change management documentation, and patch application during regular outage windows as applicable.
High Risk	• Exposes the Information System or application to a high level of risk from exploitation of an identified flaw. • Major impact on, or high risk to an Information Systems performance, network availability or data integrity is likely to occur.	Within 30 days following testing, change management documentation, and patch application during regular outage windows as applicable.
Medium Risk	• Exposes the Information System or application to a medium level of risk from exploitation of an identified flaw. • Minor impact on, or medium risk to an Information Systems performance, network availability or data integrity	Within 30 days following testing, change management documentation, and patch application during regular outage windows as applicable.
Low Risk	• Exposes the Information System or application to a low level of risk from exploitation of an identified flaw. • No impact on, or low risk to an Information Systems performance, network availability or data integrity	Apply patches within the normal patch cycle.

The following controls apply to patch management for all LegalMaps Information Systems:

9.6.1.1 Application and system administrators are responsible for software maintenance, patch management and version control of all systems and applications under their control.

9.6.1.2 Monitor vulnerability alert resources for the systems and applications supported.

9.6.1.3 Document the application of patches (i.e., using existing change control methods). Documentation must be maintained for a minimum of one year and must contain the following: system name, patch name/number, date, time the patch was applied, and the name of the person who applied the patch.

9.6.1.4 Confirm that all Information Systems and associated software maintain the latest vendor-supplied security patches. System software should be behind in version no more than a single major revision or more than thirty (30) days if such version differences pose a security or stability risk.

9.6.1.5 All software patches should be tested prior to deployment.

9.6.1.6 Proper change control procedures must be followed for the application of software updates, patches, and configuration changes.

9.6.1.7 All new, test, and development systems must be patched/updated to the latest version of patches available prior to connection with production systems.

9.7 Open Source Software

Standards regarding the use of open source software are to be set by LegalMaps Enterprise Architecture.

Open source software means any software, program, or code, regardless of language or medium of delivery (i.e., downloaded from the Internet or CD-ROM distribution) whose human-readable source code is made available for use or modification as users or programmers see fit. To be considered open source software, the license accompanying the software states that: (a) the software being distributed must be redistributed to others without restriction; (b) the source code is available so the programmer can improve or modify the software; and (c) the license can require that improved versions of the code carry a different name or version than the original code.

Policies for open source software are extensive due to timeframes of implementation and applicable requirements.

9.7.1 Review and Approval Procedures for Open Source Software

Review and Approval for Open Source Software is the responsibility of LegalMaps Enterprise Architecture and is also subject to the Security Assessment process managed by LegalMaps Security.

Any existing or proposed arrangement involving new or existing covered code may be rejected or modified by the LegalMaps Security Organization.

Individuals will be asked to provide any OSS license agreements in possession and to provide further information regarding use of OSS in the applicable area.

9.8 Internet Sites

LegalMaps Internet sites must comply with all requirements set forth in this policy.

In addition, each site must successfully pass a comprehensive set of penetration tests to prove the system is ready to go operational. Tests must validate that no malicious code or unauthorized modifications were made that may compromise the system's integrity.

9.8.1 Approvals for Internet Sites

The appropriate personnel must be notified when registering a Universal Resource Locator (URL) or when establishing an Internet site either internally or hosted by an external provider. The group of appropriate personnel includes the Director of Information Security or their delegate, the Business Unit IT Manager, Business Unit Attorney, and LegalMaps Branding group. A signoff must be obtained for each of these

sections plus a signoff from the Business Owner before the site can go live. The consolidated approval process for Internet sites also addresses concerns in seven supporting areas:

- Third Party Website Development/Hosting;
- Procurement;
- Tax Issues;
- Securities Law;
- Creative Design/Corporate Branding;
- Record Retention; and
- Web site Context and Text.

The signed forms must be filed with the Business Owner, Domain Name Registrar, and the Security Assessment Center.

9.8.2 Domain Registration

To register an address, even if it is just to keep someone else from reserving the name, the LegalMaps Domain Name Registrar must be contacted and provided with site-specific information. This should include site description, status, points of contact and other pertinent identifying information. The Registrar is responsible for keeping a database of all LegalMaps URL signed applications.

9.8.3 Trademark

To promote consistency in trademark use and marking throughout LegalMaps and its subsidiaries, it is important to remember that correct trademark use and marking should be observed on all Internet sites. Improper use can lead to loss of protection and be used against LegalMaps as evidence of descriptiveness of the trademark if involved in litigation.

9.9 Application Security Reviews

All applications must have a security review performed periodically. The exact type and frequency of security review(s) to be performed depends on a variety of factors such as how the application was developed, the criticality of the application to the organization, and the type of data the application will be handling. Please reference LegalMaps' Web Application Security Standards document for more information on application code scans and reviews.

9.9.1 Commercial/Off-the-shelf Applications

Applications that are purchased commercially must have a vulnerability scan performed both immediately prior to being placed into production as well as on a quarterly basis after implementation. At minimum, the scan must be performed using a vulnerability assessment tool approved by LegalMaps Security. It is strongly recommended that commercially-purchased applications that will be storing or processing sensitive (Level 3 or higher) data such as financial or credit card data, or classified as a High Risk application, be scanned for vulnerabilities by an independent third party approved by LegalMaps Security.

9.9.2 Custom-Developed Applications

Applications or code that are created or written for LegalMaps must have a vulnerability scan performed both immediately prior to being placed into production as well as on a quarterly basis after implementation. In addition to a pre-production vulnerability scan, any custom-developed application or code that will store, transmit, process, or support other systems that handle sensitive (Level 3 or higher) data must also have a source code security review performed prior to being placed into production. Source code security reviews

must be performed using a source code assessment utility approved by LegalMaps Security. It is strongly recommended that custom-developed applications/code handling financial or credit card data, or classified as a High Risk application, have a source code review performed by an independent third party approved by LegalMaps Security.

Software development life cycle (SDLC) activities must include procedures that support the requirement that appropriate vulnerability and source code reviews are performed, analyzed, remediated, and approved prior to code or applications being placed into production. Based on the results of a risk assessment performed on the application/code, or the purpose for the application/code if it hasn't been developed yet, LegalMaps Security might require that additional or more frequent security reviews be performed during development or after implementation.

10 Security Incident Management

10.1 Reporting Security Events

All known or suspected security vulnerabilities, weaknesses, or violations, in addition to the unauthorized disclosure of sensitive LegalMaps information, must be reported in an expeditious and confidential manner to a manager who in turn will escalate the issue to a member of LegalMaps Security whether the breach was at LegalMaps or a third party holding LegalMaps information. If the security event or incident noted relates to a user's immediate manager, then the user should report the incident to their manager's supervisor, another manager, or directly to LegalMaps Security.

Users should not, in any circumstances, attempt to prove a suspected weakness or vulnerability.

Except as required by laws and regulations, reporting security violations, problems, or vulnerabilities to any party outside LegalMaps without the prior written approval of LegalMaps Security is strictly prohibited.

Stolen or lost LegalMaps assets, such as a laptop, RSA token, or PDA, can be reported twenty four (24) hours, 365 days a year at +1 612 886 8300.

Computer security incidents involving denial of service, malicious code, unauthorized access or inappropriate use may be reported 24 hours a day, 365 days a year by calling +1 612 886 8300, or via email to admin@LegalKaizen.com.

10.1.1 Incident Definition

An incident is defined as an interruption of the business or any part of the business including processes, services, systems, etc., including both physical and logical security incidents. Some types of incidents are Information System failures, denial of service attacks, unauthorized or improper access of information, physical damage, theft, loss, property damage, bomb threats, and natural and man-made disasters, etc.

It is important that all incidents, regardless of the type or cause, be treated with the same methodical approach as outlined in this policy.

10.1.2 Incident Notification and Isolation

10.1.2.1 All users are required to be aware of the Incident Response Policy and reporting procedures. When in doubt, all associates should report all incident notifications to their direct manager.

10.1.2.2 All users are required to report incidents or suspected incidents as quickly as possible.

10.1.2.3 Procedures must be in place for managers to escalate incidents within specific timeframes.

10.1.2.4 System and network administrators will take necessary action to limit the effects of an incident by isolating and defining the problem as narrowly as possible.

10.1.3 Documenting Incidents

Critical and relevant aspects of the incident are documented and reported to appropriate personnel. Procedures must address information to be recorded, timelines for submission of reports, report recipients, details of the event, and retention of reports in a formal format.

The initial notification must provide the following information, at a minimum:

- A general description of what occurred;

- Details on whether LegalMaps or customer data was compromised;
- If appropriate, characterization of perpetrator(s) thought to be involved (i.e., insider, outsider);
- Corrective actions that have been taken or that are planned; and
- Remediation Recommendations

10.1.3.1 Reporting Incidents to Outside Agencies

Only LegalMaps Corporate Communications, under the auspice of LegalMaps Security and LegalMaps Legal counsel, may authorize the reporting of security incidents to outside agencies. These positions have the authority to delegate this responsibility on a case-by-case basis. LegalMaps Security will provide periodic updates throughout the investigation to allow for the earliest possible contacting of outside agencies when and if the security incident warrants it.

10.1.3.2 Reporting Incidents to Clients or Customers

Only LegalMaps Corporate Communications, under the auspice of LegalMaps Security and LegalMaps Legal counsel, may authorize the reporting of security incidents to clients or customers. Specific laws may require notifying clients or consumer customers. Many external standards also require notice to clients and/or consumers of security breaches. While not defined herein, procedures for proper notification under such circumstances are required and must be adhered to in accordance with the law and GLB Information Security Programs.

10.1.4 Reporting Software Malfunctions

All software malfunctions should be reported to the local departments responsible for management and administration of desktops and/or servers. Procedures should be developed to respond to software malfunctions that appear potentially malicious in nature. The following actions should be considered:

- The symptoms of the problem and any messages appearing on the screen should be noted.
- The computer should be isolated, if possible, and use of it should be stopped. Equipment is to be examined; it should be disconnected from any organizational networks before being re-powered. Diskettes should not be transferred to other computers.
- The matter should be reported immediately to the LegalMaps Security manager. Users should not attempt to remove the suspected software unless authorized to do so. Appropriately trained and experienced staff should carry out recovery.

10.2 Management of Security Incidents and Improvements

Adequate managing and improvement is crucial in today's fast-paced, ever-changing business environment. It is essential that LegalMaps and its Business Units have the ability to respond to potentially damaging incidents with a consistent and effective plan.

LegalMaps must have an established incident response team and developed procedures and plans to respond to security incidents.

10.2.1 Responsibilities and Procedures

Incident management responsibilities and procedures are required to provide for a quick, effective and orderly response to security incidents. The following guidelines outline recommended procedures for incident handling.

Procedures must be established in advance to cover all potential types of security incident, including:

- Information system failures and loss of service;
- Denial of service;
- Errors resulting from incomplete or inaccurate business data; and
- Breaches of confidentiality.

In addition to normal contingency plans (designed to recover systems or services as quickly as possible) the procedures must also cover:

- Analysis and identification of the cause of the incident;
- Planning and implementation of remedies to prevent recurrence, if necessary;
- Collection of audit trails and similar evidence;
- Communication with those affected by or involved with recovery from the incident; and
- Reporting the action to the appropriate authority.

Action to recover from security breaches and correct system failures should be carefully and formally controlled. The procedures must confirm that:

- Only clearly identified and authorized staff are allowed access to live systems and data;
- All emergency actions taken are documented in detail;
- Emergency action is reported to management and reviewed in an orderly manner; and
- The integrity of business systems and controls is confirmed with minimal delay.

10.2.2 Classification of Alert Severity Levels

LegalMaps Alert Severity Matrix	
Severity Level 1 (Critical)	Total loss of service or facility. Examples: Divisional business unit work stoppage; bomb threat, natural or man-made disasters, missed commitments to government customers or LegalMaps business partners. Total losses of critical systems or applications, general network or host outages.
Severity Level 2 (Severe)	System or application outage, degradation of a critical nature, theft or destruction of property. Examples: Line-of-business application not functioning; customer process halted; Service Level Agreement (SLA) missed; isolated network or host outage, execution of hostile code (viruses, Trojan horses, worms, etc.) on one or more protected servers, one or more intruders gaining interactive access to protected servers or network devices, theft of information or equipment or physical destruction of property..
Severity Level 3 (Warning)	Limited customer impact. Examples: Network or host degradation; data unusable; customer requested; excessive ticket transfers, repeated unsuccessful login attempts, and repeated unsuccessful file access attempts.
Severity Level 4 (Informational)	Localized alert with little or no customer impact. Examples: Call/Alert/alarm received; a non-critical workstation down; work around available. Examples are ping sweeps, port scans, and DNS zone transfer attempts.

10.2.3 Incident Classification Matrix

Characteristics	Severity			
	Category 4 (Informational)	**Category 3 (Warning)**	**Category 2 (Severe)**	**Category 1 (Critical)**

Sensitivity of Asset	Asset not Critical	Asset not Critical	Asset is Critical	Asset is Critical
Damage	No Damage	Little Damage	Moderate Damage	Major Damage
Expert Assistance	None or some Internal	Internal	Internal or External	Internal or External
Interruption of Service	None	Brief	Brief (<4 Hours)	Extended (>4 Hours)
Notify Owner	Monthly	Weekly	Immediate	Immediate
Notify Custodian	Weekly	Daily	Immediate	Immediate

10.2.4 Security Incident Database

LegalMaps Security shall maintain a comprehensive database of company-wide security incidents for tracking and historical review purposes.

10.2.5 Completing the Security Incident Report

LegalMaps Security personnel responsible for identification of an incident are responsible for completing a Security Incident report containing all pertinent information regarding the security incident by the completion of the next business day. Security Incident Reports will be further reviewed by the Director of Information Security and the Corporate Security Council.

10.2.6 Learning from Security Incidents

There should be mechanisms in place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored. This information should be used to identify recurring or high impact incidents or malfunctions. This may indicate the need for enhanced or additional controls to limit the frequency, damage and cost of future occurrences, or to be taken into account in the security policy review process.

10.2.6.1 Incident Follow-Up

LegalMaps Security will track resolution of incidents and follow up on any pending corrective actions. Upon completion of the security investigation, a lessons learned with all relevant departments will be conducted. Planning and implementation of remedies to prevent reoccurrence will be implemented in all cases.

10.2.7 Collection of Evidence

Audit trails and similar evidence should be collected and secured, as appropriate, for:

- Internal problem analysis.
- Use as evidence in relation to a potential breach of contract, breach of regulatory requirement or in the event of civil or criminal proceedings, e.g. under computer misuse or data protection legislation.
- Negotiating for compensation from software and service suppliers.

11 Business Continuity Management

It is reasonable and prudent to guard against potential disasters and prepare plans that will enable the business areas to recover from such disruptions and resume business functions in a timely fashion.

It is critical to note that Business Continuity is the overarching function such that a business can recover and/or resume business functions in the event of a crisis/disaster. There are multiple elements of Business Continuity that account for the people, the technology and the business functions themselves.

- Emergency Response is the plan that provides for the safety of the people and helps drive to a decision on response and recovery.
- The Business recovery is the plan that supports the business processes.
- Disaster recovery is the plan that addresses the technology recovery and staff required to support this technology. This responsibility lies within the LegalMaps Security organization in partnership with the LegalMaps facilities management team.

The objective of this Business Continuity policy is to provide a framework within which the individual business areas and LegalMaps as a whole can achieve:

- Prevention – controls to minimize the probability of business interruptions
- Response – initial reaction to the crisis; determines impact of the crisis and decision for next steps; invokes crisis management
- Resumption – steps to resume critical business functions; invokes disaster recovery and business recovery plans
- Recovery – steps to recover to normal business while operating in recovery mode.
- Restoration – steps to restore business as usual in the original site or at a new facility.

11.1 Business Continuity

LegalMaps' Business Continuity processes are established by LegalMaps Security organization in partnership with the LegalMaps facilities management team.

The following general guidelines apply to LegalMaps and its subsidiaries. It should also serve as a guideline for evaluating the Business Continuity (BC) plans of any and all business partners with which LegalMaps conducts or will conduct business.

11.1.1 Responsible Party for Business Continuity Plan

All organizations within and LegalMaps as a whole must assure that there is an appointed responsible person within each organization (as well as LegalMaps as a whole) charged with the responsibility of developing, maintaining, and periodically testing the Business Continuity. Disaster Recovery plans are developed, owned and maintained by the LegalMaps Security group, but are based on requirements provided by the business

11.1.3 Conditions for Activating Business Continuity Plan

All organizations, and LegalMaps as a whole, must include in their plans conditions for activating any part of the plan, and the responsible parties involved in plan activation. LegalMaps Security should be notified of all plan activations.

11.1.4 Analysis and Review of Business Continuity Plan

Each BC plan must be based on a Business Impact Analysis (BIA) that is conducted or reviewed on a regular basis. The BIA helps determine whether business-as-usual operations should be modified and forms the basis for the resulting BC plan strategies: respond, resume, recover and restore:

- The Respond Strategy entails the actions required to invoke Crisis Management and determine the next steps based on the impact of the crisis.
- The Resume Strategy provides the necessary actions required to resume the critical activities. Note that these steps may include employees working from home or other employees performing the critical functions in lieu of.
- The Recover Strategy provides actions that target to get normal operations up and running again while in a temporary operation mode.
- The Restore Strategy provides steps to finally restore business as usual at the original site or a new facility.

11.1.5 Communication Plan

A Communications plan will identify actions to be taken to confirm that Senior Leadership Team, staff, and external media sources (if necessary) are kept informed throughout the process, and especially, of any incidents which will require their direct intervention or decision.

11.1.6 Maintenance

A Maintenance plan will identify action to be taken such that BIA and all plans (BC, Crisis Management, and Disaster Recovery) are updated and kept current in a timely fashion.

11.1.7 Testing the Plan

Various testing scenarios will identify actions to be taken to confirm that the plans are viable and must document all activities to provide for end-to-end recovery capabilities.

11.1.8 Awareness

Awareness combined with management's direction will support the requirements that all associates be aware of the plans and what they may be called upon to perform in the event of an interruption.

11.2 Business Continuity Management Process

There must be a centralized, managed process in place for developing and maintaining business continuity throughout the organization. It should bring together the following key elements of business continuity management:

- Understanding the different types of interruptions and the risks the organization is facing in terms of their likelihood and impact, including an identification and prioritization of critical business processes;
- Considering the purchase of suitable insurance which forms part of the business continuity process;
- Formulating and documenting a business continuity strategy consistent with the agreed business objectives and priorities;
- Formulating and documenting business continuity guidelines in line with the agreed strategy; and
- Regular testing and updating of the plans and processes put in place.

11.2.1 Business Continuity and Risk Assessment

Business continuity will begin by identifying events that can cause interruptions to business processes (i.e. equipment failure, flood, and fire due to natural or man-made threats) and the impact of those interruptions (financial, legal, etc over a period of time). The Business Impact Analysis (BIA) is a tool used to identify both risks and impacts. Owners of business resources and processes are responsible for completing this survey. The assessment considers all business processes, is not limited to the information processing facilities, and will identify risk events according to area hazards and prioritize response accordingly. Key outcomes of the BIA are the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each process. The RTO is the deadline for pre-defined systems, applications, processes, etc to be restored and available for end users (internal and external). The RPO is the point in time that systems/data must be recovered after an outage. This survey will guide the overall strategy to the business continuity plan.

11.2.2 Writing and Implementing Continuity Plans

Plans must be developed to maintain or restore business operations in the required time scales following interruption to, or failure of, critical business processes. The business continuity planning process should consider the following:

- Identification and agreement of all responsibilities and emergency procedures;
- Implementation of emergency procedures to allow recovery and restoration in required time-scales. Attention needs to be given to external business dependencies and the contracts in place;
- Documentation of agreed procedures and processes;
- Appropriate education of staff in the agreed emergency procedures and processes including crisis management; and
- Testing and updating of the plans.

11.2.3 Business Continuity Planning Framework

A single framework of business continuity plans is maintained to confirm that all plans are consistent, and to identify priorities for testing and maintenance. Each business continuity plan should specify clearly the conditions for its activation, as well as the individuals responsible for executing each component of the plan. When new requirements are identified, established emergency procedures, e.g. evacuation plans or any existing fallback arrangements should be amended as appropriate.

A business continuity planning framework requires the following:

- The conditions for activating the plans which describe the process to be followed (how to assess the situation, who is to be involved, etc.) before each plan is activated;
- Emergency procedures that describe the actions to be taken following an incident that jeopardizes business operations and/or human life. This should include arrangements for public relations management and for effective liaison with appropriate public authorities, e.g. police, fire service and local government;
- Fallback procedures which describe the actions to be taken to move essential business activities or support services to alternative temporary locations, and to bring business processes back into operation in the required time-scales;
- Resumption procedures which describe the actions to be taken to return to normal operations;

- A maintenance schedule which specifies how and when the plan will be tested, and the process for maintaining the plan;
- Awareness and education activities which are designed to create understanding of the business continuity processes such that the processes continue to be effective;
- The responsibilities of the individuals, describing who is responsible for executing which component of the plan. Alternatives should be nominated as required;
- A policy should exist which details the responsibilities of management to provide for the timely resumption of critical business functions in the absence of normal services following a major interruption of information services;
- Information availability threat analysis and risk evaluations must be undertaken and compensating measures identified. These factors are periodically reassessed to consider the impact of changes in the business and systems environments;
- The critical business processes must be analyzed to identify vital information supporting systems and facilities and to determine the impact of their financial and operational loss to the business;
- Recovery strategies and goals must be consistent with the level of risk the organization faces and the business impacts of loss are weighed against the cost of recovery. Minimum recovery resources of this recovery strategy have been identified to support the critical business functions and have been approved by senior management; and
- A backup program for critical/vital information and materials, covering on-site and off-site storage, must be in place and effectively managed.

Each plan should have a specific owner. Emergency procedures, manual fallback plans and resumption plans should be within the responsibility of the owners of the appropriate business resources or processes involved. Fallback arrangements for alternative technical services, such as information processing and communications facilities, should be the responsibility of the service providers.

11.2.4 Testing, Maintaining, and Re-Assessing Business Continuity Plans

Business continuity plans may fail on being tested, often because of incorrect assumptions, oversights, or changes in equipment or personnel. They should therefore be tested on an annual basis to confirm that they are up to date and effective. Such tests should also confirm that all members of the recovery team and other relevant staff are aware of the plans.

12 Compliance

12.1 Compliance with Legal Requirements

Compliance with all security policies and applicable laws, regulations and standards as outlined in Appendix A *Relevant Laws, Regulations and Standards* must be followed to avoid breaches of any criminal and civil law, statutes, regulatory or contractual obligations or applicable security standards or rules.

The design, operation, use and management of Information Systems may be subject to statutory, regulatory and contractual security requirements.

Advice on specific legal requirements should be sought from the LegalMaps Legal Counsel's Office, in conjunction with LegalMaps Security, which shall make the determination whether outside legal advisors should be consulted. Legislative requirements vary from country to country and may impose legal restrictions on information created in one country that is transmitted to another country (i.e. trans-border data flow).

12.2 Identification of Applicable Legislation

All relevant statutory, regulatory and contractual requirements should be explicitly defined and documented for each Information System. The specific controls and individual responsibilities to meet these requirements should be similarly defined and documented for each Information System. LegalMaps Legal Counsel, in conjunction with LegalMaps Security, is responsible for assignment and review of all applicable legislation, laws, and regulations that apply to each Information System.

12.3 Intellectual Property Rights (IPR)

Appropriate procedures to validate compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products are as follows:

12.3.1 Patent

LegalMaps' pending patent applications or any inventions not covered by any of LegalMaps' patent applications are considered trade secret information and should not be disclosed to third parties.

It is important to remember that correct patent marking should be observed on all products and Information Systems. For products that are covered by the claims of one of LegalMaps' issued patents, the patent number should be clearly marked on the marketing materials, the product and the packaging. For products that are covered by the claims of one of LegalMaps' pending patent applications, the marketing materials, the product and the packaging should be stamped with the phrase "Patent Pending." It is important to note that the patent application must be filed with the U.S. Patent and Trademark Office before marking any item with "Patent Pending." If any questions regarding marking or patent issues arise, please contact the Intellectual Property Legal Group of the LegalMaps Legal Department.

12.3.2 Copyright

Legislative, regulatory and contractual requirements place restrictions on the copying of proprietary materials as well as on the copyrighted materials of third parties. Only non-sensitive or non-proprietary material that is developed by LegalMaps, or that is licensed to LegalMaps, should be used. If there is any doubt as to whether copyrighted material should be used, please contact LegalMaps Legal Department.

12.3.3 Trademark

To promote consistency in trademark use and marking throughout LegalMaps and its subsidiaries, it is important to remember that correct trademark use and marking should be observed on all Information Systems. Improper use can lead to loss of protection and can be used against LegalMaps as evidence of improper use of the trademark if involved in litigation. The Trademark Administration group, or Trademark Legal Analyst, should review all advertising in the proof stage to verify that existing trademarks are being used in the proper fashion. Before new trademarks are adopted, the Intellectual Property Legal Group, the LegalMaps Legal Department should perform a Trademark Clearance analysis. If any questions regarding marking or trademark issues arise, please contact the Intellectual Property Legal Group of the LegalMaps Legal Department.

12.3.4 Trade Secret

All employees, contractors and consultants are required to protect LegalMaps owned information against deliberate, unintentional, inappropriate, or unauthorized disclosure. All trade secret information should be marked with confidentiality notices. There shall be no disclosure of LegalMaps trade secrets to anyone outside LegalMaps until an authorized representative of the proposed recipient and LegalMaps have formally signed a non-disclosure agreement. All employees, contractors and consultants are forbidden to:

a) Illegally use the trade secrets of others;

b) Violate terms of any legally binding license agreement relating to the intellectual property of LegalMaps or others; or

c) Attempt to acquire the trade secrets of others by improper or unethical means.

If any questions regarding marking or trade secret issues arise, please contact the Intellectual Property Legal Group in the LegalMaps Legal Department.

12.3.5 Software Copyright

Proprietary software products are supplied under a license agreement that usually limits the use of the products to specified machines and may limit copying to the creation of back-up copies of the software. The following controls are required to provide for software copyright compliance:

a. Issuing standards for the procedures for acquisition of software products;
b. Maintaining proof and evidence of ownership of licenses, master disks, manuals, etc.;
c. Maintaining proof and evidence of compliance with non-disclosure obligations;
d. Implementing controls to confirm that any maximum number of users permitted is not exceeded;
e. Carrying out periodic audits to confirm that only authorized software and licensed products are installed; and,
f. Complying with terms and conditions for software and information obtained from public networks.

12.3.6 Protection of Organizational Records

LegalMaps must confirm that access to LegalMaps Data is secured against illegal or unauthorized use.

Users may have access to confidential information which we, as trusted custodians, are obliged to keep confidential and private. Users must treat all information as confidential unless you have been advised otherwise.

Specifically:

- No user of LegalMaps may permit any unauthorized person to have access to files, letters, papers, computer media, or any other database or system belonging to or relating to LegalMaps or its clients. Neither may users, either during or after the termination of their employment with LegalMaps, divulge or communicate to any unauthorized person any information or knowledge of a confidential nature which they may receive or obtain in relation to the business affairs of LegalMaps except by order of a court of law.
- LegalMaps databases contain confidential data. Consequently, we must take all necessary steps to prevent the misuse of such information and the information we hold should not be used except for legitimate business reasons and for the purpose for which it was acquired.
- There may be occasions when you are asked to access the system for demonstration purposes. In doing so, information might be obtained about people you know or on behalf of people you know. LegalMaps takes a serious view of such unauthorized use of the system and only training data should be used for demonstration purposes.
    - No live data should be accessed for demonstration or training purposes. Test Data is set up for this purpose.

Users must not:

- Use systems to check your own, your family's or your friends' consumer records.
- Provide information to anyone else who may ask for it unless you have been given specific authority by LegalMaps Security.

Any access to live Consumer data must be supported by valid documentation. Examples of valid documentation include:

- A change management record for the resolution of client system problems.
- A letter from a consumer querying data relating to him or her.

Users should record each instance of access to live data on a live data approval form and these completed forms should be approved by line management.

Unauthorized use of the system in the ways noted above is considered to be Gross Misconduct and, as such, offenders will be summarily dismissed. After termination of employment LegalMaps may pursue appropriate legal action.

Access to all Consumer data creates an audit trail that is validated against the supporting documentation by a member of the LegalMaps Security team. Regular audits will be carried out to confirm that users comply with the above. All instances where data has been accessed without appropriate authorization will result in disciplinary action.

12.3.7 Data Protection and Privacy of Personal Information

A number of countries have legislation placing controls about the processing and transmission of personal data (generally information about living individuals who can be identified from that information). Such controls may impose duties on those collecting, processing and disseminating personal information, and may restrict the ability to transfer that data to other entities.

Please refer to Appendix A, *Relevant Laws and Regulations* for more information.

12.3.8 Privacy Requirements for Internet Sites

All Internet Web sites of LegalMaps and its subsidiaries must have a privacy policy that has been approved by the LegalMaps Legal. The business policies and practices related to the site must be consistent with LegalMaps Privacy Principles. Generally, if personal information is collected on a Web site, the consumer must be given notice of what information is collected, how it will be used, and an opportunity to opt-out of the use of the information for certain marketing purposes.

12.3.9 Prevention of Misuse of Information Processing Facilities

For processing facilities, management should authorize their use. Any use of these facilities for non-business or unauthorized purposes, without management approval, should be regarded as improper use of the facilities. If such activity is identified by monitoring or other means, it should be brought to the attention of the individual manager concerned for appropriate disciplinary action.

12.3.10 Regulation of Cryptographic Controls

Cryptography and cryptographic controls will be used in compliance with all relevant agreements, laws, and regulations. If activity is identified that is not authorized or where cryptographic controls have been broken or misused, it should be brought to the attention of LegalMaps Security.

12.4 Compliance with Security Policies & Standards, and Technical Compliance

Security policy compliance and enforcement is a critical component to any security program. Without compliance and enforcement, a policy may have little to no effect on the LegalMaps Security posture. Compliance and enforcement is controlled by several factors; the first being user awareness and education followed by audit, review, and subsequent sanctions. Incident reporting and forensic analysis are equally important, but often provide awareness only after an event has occurred prompting remediation.

LegalMaps resources are only to be used for LegalMaps sanctioned activities in support of LegalMaps business. Any other use must be approved by management and must not interfere or compete with LegalMaps business and must not involve any incremental cost to LegalMaps. Compliance auditing of hardcopy, softcopy or online information will be performed on an ad-hoc basis by the LegalMaps Security team and internal audit (or their delegate) to confirm compliance with corporate policies and legislation.

To confirm appropriate use of resources, a users privacy relating to electronic, telecommunications or other media, on-line activities while on LegalMaps property or utilizing LegalMaps resources (on or off site) is not guaranteed and an individual should not infer any privacy with regard to such utilization.

12.4.1 Compliance with Security Policy

Managers and LegalMaps Security shall confirm that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards. Users must comply with all policies, procedures, and standards outlined in this policy.

In addition, all areas within the organization must be considered for regular review to confirm compliance with security policies and standards. These shall include the following:

- Information Systems (Applications, Processes)
- Systems Providers
- Owners of information and resources
- Users

- Management

Owners of Information Systems shall support regular reviews of the compliance of their systems with the appropriate security policies, standards and any other security requirements.

12.4.2 Sanctions for Non-Compliance

Failure to comply with this policy may subject the user in question to disciplinary action up to and including termination of employment. Human Resources and management of users determines the final sanctions for non-compliance.

12.4.3 Technical Compliance Checking

Information Systems shall be regularly checked for compliance with security implementation standards.

Security Compliance is the enforcement engine for all LegalMaps Security policies and may perform random audits for Information Systems. A third party technical auditor may substitute for Security Compliance as deemed necessary.

All applicable LegalMaps Security policies will serve as the basis for recurring audits of all Information Systems. Information System audits must confirm that the system meets the stated security controls and all applicable LegalMaps Security policies. Additionally, Security Compliance must report on any discrepancies and assign a remediation/mitigation plan with deadlines for completion.

12.4.3.1 Technical Audit Frequency

Information Systems should be regularly checked for compliance with security implementation standards. Technical compliance checking involves the examination of operational systems to confirm that hardware and software controls have been correctly implemented. Audit frequencies are based on the classification of the Information System and its associated risk. Audits performed by LegalMaps Security Compliance will be completed as deemed necessary and not on a scheduled basis. Random audits of LegalMaps Information Systems are to be performed at the discretion of Security Compliance and have been authorized to be performed at any time and with limited notice to Information System (asset) owners.

12.5 Information Systems Assessment Considerations & Controls

All LegalMaps Information Systems not currently in production require a risk assessment to be conducted prior to production operations. The objective of the ensuing testing is to identify network and system security exposures of the networked environment, determine the effectiveness of security controls, and provide recommendations or requirements to mitigate risks.

LegalMaps Security will conduct and manage the comprehensive testing necessary to assess the sufficiency of data security controls on LegalMaps information systems.

Assessment of systems security by means of automated or manual security scanning techniques such as vulnerability scanning or penetration analysis may only be conducted under the following guidelines:

- Only authorized personnel or contracted third parties with required legal agreements may perform security analysis of LegalMaps Information Systems.
- When conducting analysis from networks not wholly owned by LegalMaps, the owners of such networks must grant approval in writing, whether it is a partner corporation or Internet Service Provider, prior to any analysis activities.

12.5.1 Attack and Penetration Testing

Periodic testing of LegalMaps Information Systems will identify existing and potential weaknesses that must be immediately mitigated. To validate the accuracy and effectiveness of this testing, it may be necessary to utilize resources from both external and internal sources.

LegalMaps Security will use state-of-the-art commercial tools to assist in identifying and addressing technical vulnerabilities. These tools search for known vulnerabilities used by hackers and provide detailed assessments of the network's communication services, operating systems, applications, and routers.

The results will be a report containing the detailed description of findings including vulnerabilities identified, evaluation of risk level, impact of threat, likelihood of exploitation, and technical recommendations. In addition, the effectiveness of the targeted intrusion detection/prevention system protecting the web environment will be examined to determine if the controlled attacks were properly identified and logged. LegalMaps Security will assist staff from the targeted system in generating a comprehensive plan of repair actions to include prioritization, completion dates, and follow-up testing to validate corrective steps taken. High-risk vulnerabilities that pose a significant threat should be addressed immediately.

12.5.1.1 IP Validation

The IP addresses that are provided will be validated so that the assessor does not scan the wrong network. Validation can avoid the serious issues that can arise from scanning a network without authorization. Source addresses must be documented and coordinated with the LegalMaps Security team prior to scanning activities.

12.5.1.2 Vulnerability Mitigation Requirements

- The Information System owner is responsible for presenting a plan of action that details all vulnerabilities and planned mitigation with deadlines within fifteen (15) days of identification.
- All vulnerabilities found and labeled as high risk during a security assessment must be mitigated or resolved within fifteen (15) days of notification.
- All other mitigation activities including security exception approvals must be addressed within a maximum of ninety (90) days from the time of vulnerability identification.

12.5.2 Protection of System Audit Tools

Access to system audit tools, i.e. software or data files, must be protected to prevent any possible misuse or compromise. Such tools should be separated from development and operational systems and not held in tape libraries or user areas, unless given an appropriate level of additional protection.

12.5.3 Intrusion Monitoring, Incident Reporting, and Forensic Analysis Requirements

Intrusion monitoring, incident reporting and forensic analysis requirements are based on the classification and type of Information System in question. Information Systems with a data classification level of Class 3 or above require intrusion monitoring services. Along with intrusion monitoring, incident reporting and subsequent forensic analysis is required as dictated by this or other more restrictive policies.

Appendix A: Relevant Laws, Regulations and Standards

- **Payment Card Industry (PCI) Security Standard,** defines a standard of due care and enforcement for protecting sensitive information. Because the payment industry places a high priority on maintaining the confidentiality and integrity of account and personal data, the PCI requirements are directed to all entities that store, process, or transmit cardholder information. The program ensures the annual validation of merchants and all service providers on both the Issuing and Acquiring side of the business. http://www.pcisecuritystandrards.org
- **Gramm Leach Bliley Act (GLBA)** The GLB Act gives authority to eight federal agencies and the states to administer and enforce the Financial Privacy Rule and the Safeguards Rule. These two regulations apply to “financial institutions,” which include not only banks, securities firms, and insurance companies, but also companies providing many other types of financial products and services to consumers.
- **Sarbanes-Oxley Act of 2002** otherwise known as the Public Company Accounting Reform and Investor Protection Act, the Act mandated a number of reforms to enhance corporate responsibility, enhance financial disclosures and combat corporate and accounting fraud, and created the "Public Company Accounting Oversight Board," also known as the PCAOB, to oversee the activities of the auditing profession. http://www.law.uc.edu/CCL/SOact/soact.pdf
- **The Freedom of Information Act/Privacy Act of 1974** which has been in effect since September 27, 1975, can generally be characterized as an omnibus "code of fair information practices" that attempts to regulate the collection, maintenance, use, and dissemination of personal information by federal executive branch agencies. While not applicable to private businesses, the Privacy Act is often utilized as a reference for the privacy and protection of non-government information as well.
- **Electronic Signatures in Global and National Commerce Act, “Digital Signature Act”** With some exceptions, E-SIGN permits the use and establishes the legal validity of electronic contracts, electronic signatures, and records maintained in electronic rather than paper form. It governs transactions relating to the conduct of business, consumer, or commercial affairs between two or more persons.
- **American National Standards Institute (ANSI) X9.79, *Public Key Infrastructure Practices and Policy Framework***
- **Common Criteria 2.1** Common Criteria establishes guidelines for secure system/application development and is best used as a guideline for purchasing secure products that attempt to maintain a specific level of security as defined by CC2.1. http://csrc.nist.gov/cc/
- **The National Institute of Standards and Technology (NIST)** dictates standards for the information technology and security industry and the U.S. Government. References within this policy may refer to publications by NIST.
- **Federal Information Processing Standards**

http://csrc.nist.gov/publications/fips/

  - Federal Information Processing Standards (FIPS) 140-2 Encryption
  - Federal Information Processing Standards (FIPS) 182-2 Digital Signature

- **Various state credit reporting laws**
- **Personal Information and Electronic Documents Act (PIPEDA)** is a Canadian law relating to data privacy. PIPEDA governs how private-sector organizations collect, use and disclose personal information in the course of commercial business. In addition, the Act contains various provisions to facilitate the use of electronic documents. PIPEDA was passed to promote consumer trust in electronic commerce. The act is intended to reassure the European Union that Canadian privacy laws are adequate to protect the personal information of European citizens. PIPEDA incorporates and

makes mandatory provisions of the Canadian Standards Association's Model Code for the Protection of Personal Information, developed in 1995.

- **Safe Harbor Program** The US Department of Commerce created the Safe Harbor certification program in response to the 1995 Directive on Data Protection (Directive 95/46/EC) of the European Commission. Directive 95/46/EC declares in Chapter IV Article 25 that personal data may only be transferred from the countries in the EEA to countries which provide adequate privacy protection. Historically establishing adequacy required the creation of national laws broadly equivalent to those which implemented Directive 95/46/EU in Europe. Although there are exceptions to this blanket prohibition (for example where the disclosure to a country outside the EEA is made with the consent of the relevant individual - Article 26(1)(a)), they are limited in practical scope.