Information Security Policy

Purpose:

The purpose of this Policy is to establish the requirements and management expectations for protecting the organization's Confidential information systems and assets.

Applies to:

All computer and network systems, software, and paper files owned by and/or administered by the Organization, (Computer and network systems include, but are not limited to, the following items owned or leased by the Organization, and used by the Organization personnel for information access: servers, storage systems, personal or laptop computers, network equipment, telecommunications systems and mobile devices. Software includes operating systems, databases, and applications, whether developed by then Organization or purchased from software vendors, or shareware/freeware in use within production systems), all Organization employees worldwide, except where compliance with this policy would violate any law or regulation in the country where the subject is located, and components listed above that are managed or administered by third parties for the organization. Third parties include consultants, contractors, temporary workers, service providers, or business partners who access company system resources.

Definitions:

Please refer to Information Security Policies or Standards Definition, Organization *Definitions Policy* for applicable definitions.

Policy:

I. Security Program Management:

A. Information Security Program

a. This Information Security Policy outlines the responsibilities and expectations for security of information assets and information owned, held or licensed by the Organization. The controls described in this Policy are collectively known as the Organization's Information Security Program, which is designed to reflect the Company's business objectives, prevent the unauthorized use of or access to our information and information systems, and maintain the confidentiality, integrity, availability and resilience of information.

b. The Policy is guided by business and regulatory requirements specific to our business, and industry standards for information security and privacy. Specific business projects may require compliance with specific standards or directives pertinent to special categories, sensitive or classified information. A list of applicable laws, directives, and standards is maintained by the Policy owner.

c. The Information Security Policy describes the general controls and requirements for all areas of the Program, but references and links to other documents provide a greater level of detail. These documents, and the Enterprise Policy Manual, are part of the terms and conditions of employment with Organization and are acknowledged at the time of initial employment and annually thereafter. External parties, including contractors, consultants, or temporary personnel working for the Organizaiton, must be provided with this Policy, and

other applicable policies or procedures, by the sponsoring business area or employee.

B. Security Organization
    a. The Information Security organization is designed as a distributed model with central oversight and governance. Led by the Organization Chief Information Officer (CIO), Information Security team (IS) coordinates the global Security Program and has primary responsibility for information and physical security. Security support for the business areas is represented by designated roles, with some consultants and non-employees who may also have security responsibilities.
    b. Governance is through a Risk Management Committee led by senior management and meeting at least bi-annually. The Committee consists of the heads of Information Technology (IT), Compliance, Legal, Finance, International Services and the President of the Firm. This forum provides a collaborative link and reinforcement of Information Security and Privacy issues across Organization locations and business areas.
    c. IS maintains ongoing contact with security groups, technical experts, and peer groups of security professionals in similar organizations to help augment and guide their efforts.
    d. Everyone who uses the Organization's systems and networks, or has access to Organization information, shares in the responsibility for its protection as demonstrated and acknowledged through the Organization's

C. Information Technology Architecture
    a. Information Security has the mission of providing risk-based security guidance through collaboration with the business and our clients. Working with other IT teams focusing on data analytics, emerging technologies, portfolio optimization, and core infrastructure technology, IT seeks to promote trust and assurance through advanced technologies and innovative methods.
    b. Increasingly, modern IT environments rely less upon central control of all information resources and more on collaboration with internal business areas or external cloud and infrastructure service providers. The Organization's Information Security Program reflects this and seeks to ensure that our technology architecture meets compliance, regulatory, and privacy requirements. Systems are designed with a defense-in-depth security approach, supplier diversity, and sustainable systems management. As appropriate, alignments are made with Federal critical infrastructure protection programs and standards.
    c. IT maintains a variety of inventories of system and information assets in support of reporting and ongoing assurance or accountability. These include servers and infrastructure components, license information, and physical locations.

D. Risk Management
    a. IT's Risk Management Program is coordinated by Information Security and is designed to identify, assess, treat, and monitor information security risks. The assessment of risks takes into account three sources when risks are identified and require mitigation: (i) the overall Organization business strategy and objectives; (ii) applicable regulatory or contractual requirements; and

(iii) the requirements for information handling within the technology architecture. A Risk Register is maintained to track and monitor information security risks across the business.

E. Information Classification

a. The Organization categorizes information regardless of medium (paper or electronic) according to its sensitivity and the potential impact of disclosure. Please refer to Organization Information Risk Classification Policy for more details. Business Application Owners are responsible for working with Organization IT compliance and Privacy Professionals to determine the appropriate classification level for the information contained within the respective applications they manage for the business. Information Security will provide appropriate security technology solutions (such as encryption) for electronically stored information where this level of protection is required. Organization information is classified into four categories:

1. **Non-Confidential** (e.g., Public Information or Non-Personal Information)
2. **Confidential** (e.g., Restricted Information or Personal Information)
3. **Highly Confidential** (e.g., Intellectual Property, Proprietary and Attorney Privileged Information, Client Information or Special Category Personal Information)

b. For further guidance, information, and specific category handling, standards are described in the Organization *Information Risk Classification Policy and Organization Information Risk Classification Standard*

II. Personnel and Training

A. Human Resources

a. The Human Resources (HR) department initiates the addition of new employees and contractors, and performs other essential security-related functions, including recruiting, maintaining position risk descriptions, performing background screening, transfer and termination activities, and sanctions. Non-U.S. employees are managed by local Human Resources representatives.

B. Acceptable Use

a. The Organization's information and technology resources must be used in an approved, ethical, and lawful manner. Employees and contractors must always be alert to actions and activities they may perform that could breach the Organization's Enterprise Policy Manual which details specific rules of behavior regarding the Internet, electronic mail, use and access of Organization computing resources and Organization Confidential Information.

b. All suspected or identified policy violations, system intrusions, and other conditions that might jeopardize the Organizations information or systems must be immediately reported. If users have any doubt or queries on the appropriateness of their actions, they should clarify their understanding with their manager or contact *Information-Security@organization.com* for guidance. Users who deliberately violate information security policies will be subject to disciplinary action up to and including termination from employment or association with the Organization, in accordance with applicable laws and regulations.

C. Screening
    a. Employees are subject to pre-employment background screening that may include criminal, credit, and reference checks, in accordance with applicable laws and regulations. Screening is performed prior to provision of access to information systems and will reflect the requirements of the assigned position. Those staff members and others working on critical projects related to national security may require additional personnel screening, including clearance(s) if required.

D. Access Administration
    a. Initial access is requested through HR workflow and processes which will notify the appropriate Office Coordinators (OCs) and access administrators in IT and business areas. New hires must sign a confidentiality agreement and other documents as part of the terms and conditions of employment. Nightly feeds alert administrators of the current access roster so that changes or transfers can be processed. Managers must follow termination procedures available on Corporate WebSite when a worker is no longer associated with the Organization. Additional guidance on access controls and requirements can be found in the Organization *Access Control Policy.*

E. Security Awareness and Training
    a. The Employee Education Department within Human Resources coordinates enterprise training through Organization University. Specific courses that include privacy and security awareness are required for all employees. A Learning Management System application tracks courses taken and required renewals.
    b. Continuous reinforcements for security awareness are provided regularly by Information Security through internal social media, newsletters, and targeted phishing education campaigns. As appropriate, role-based training for those with assigned security roles and responsibilities will be provided. The *Organization Awareness and Training Policy* outlines additional training requirements for all Organization staff.

F. Email and Messaging
    a. All Data Users who communicate by using Organization-owned electronic mail (email) and messaging systems are responsible for exercising due care when using these systems, using email and messaging only for legitimate purposes, and using only approved technologies for instant messaging and chat with both internal and external colleagues. Data Users should also be aware at all times of the Information classification of data contained in communication media that is associated with Organization business affairs. Review the Organization *Email and Messaging Policy* for additional requirements.

G. Third-Party Security
    c. Sponsoring managers request access for consultants or contractors by submitting a Subcontractor Account Request form through Assist. Once approved, an email is sent to the consultant, requiring him/her to agree to confidentiality and other requirements

a. be issued permanent badges prior to their start date. Managers must notify HR if the worker will not be renewed and confirm termination details prior to the separation date.
b. The goal of third-party risk management processes is to ensure that potential information risks associated with these external parties (suppliers, vendors, and service providers) are identified, assessed, and managed. The sponsoring Organization employee is responsible for identifying risks associated with the external entity prior to engagement. Reasonable security measures, commensurate with the level of risk, must be maintained by third parties. All third parties must agree contractually to comply with applicable laws, implement mutually agreed safeguards, and to maintain confidentiality. Information Security maintains an inventory of Service Provider or third-party providers and the processes to assess, mitigate, or accept identified risks.

III. Access Control

A. Access Control Principles
   a. Access to Organization systems and applications is role-based and is granted to authorized users utilizing the following principles:
      1. Information is available only to those with a legitimate need-to-know. Access is provided based on job requirements and data classification.
      2. Separation of duties is implemented as appropriate, with tasks and privileges shared among multiple individuals.
      3. Users will be restricted to the least access privileges necessary to perform their assigned job.

B. Authorization Processes
   a. Designated Business Application Owners are in place to ensure that appropriate decisions are applied to each request. Their or a delegate's approval is required to gain access to applications or to gain specific privileges. Most approvals are tracked through the IT Support ticketing system, but some requests may be tracked through specialized applications or forms. Additional requirements can be found in the Organization *Access Control Policy*.

C. Account Management
   a. The Organization utilizes automated provisioning to create and disable user accounts. All users and identifiers must be unique. External users (contractors and consultants) are maintained separately from the primary HR system of record. Non-interactive accounts (e.g., for systems, services, applications) are tightly controlled and reviewed periodically. The ability to access information must be made based on positive identification rather than solely by any security attributes associated with an individual.

D. Account Rules
   a. Automatic enforcement of access control roles is implemented wherever possible. Active Directory (AD) domain account policy is configured to automatically lock accounts after a defined number of invalid access attempts. Re-authentication by the Service Desk is required. Sessions lock automatically after a period of 25 minutes of inactivity.

E. Authentication

a. The minimum level of user authentication is a password. System and organizational controls are in place to enforce the selection of strong passwords. Password requirements include length and complexity, password history, system lockout, and prohibition of password sharing.
b. IT Administrators utilize a password management tool for safe storage of sensitive passwords and must use a separate account to perform privileged actions, different from their normal user account.
c. Procedures are in place for initial distribution and ongoing management of authenticators (e.g., passwords, key cards/badges). These include requirements such as changing of vendor default passwords, establishing account time restrictions, password / badge expiration and re-authentication, and user safeguards for protecting these authenticators. Depending on the application, feedback regarding failed access attempts that could allow unauthorized individuals to compromise authentication mechanisms is not provided. The Organization *Password Policy* provides additional requirements for password use, protection and maintenance.

IV. Physical Security

A. Physical Security Controls

a. Information protection is dependent on adequate physical security. All Organization sites employ physical access control measures to ensure that the company's facilities and assets remain secure. International facilities are managed locally, generally coordinated by Office Security Group or equivalent staff.
b. Each Organization site is protected by entry controls designed to allow only authorized personnel to obtain building and floor access. Each site may have different procedures for entry, with building management issuing badges / access cards for site access. Badges are assigned to individuals, disabled when no longer authorized, and purged prior to reuse. Access to floors, offices, and secured interior rooms is integrated into a single badge access control system maintained by Information Security. Telecom closets, data center and equipment rooms are protected by an additional level of card key authorization. Printers, output devices, and distribution areas are always housed within secure areas that may require an additional level of card access.
c. Visitor requirements vary by site. At most sites, visitors must sign in at a reception desk and be authorized for further access by the sponsoring Organization employee. Visitors must be escorted or supervised at all times while on premises.
d. Physical access to facilities and secured areas is monitored by the use of video cameras, maintained by Information Security. Video data is stored and retained in compliance with local laws and regulations.
e. Facilities and/or Office Security Group have designated staff at each site who are responsible for participation in emergency response efforts, fire drills, and handling safety concerns.

B. Environmental Protection

a. Primary data centers are located in third-party hosting centers with data center environmental systems managed by those providers. Organization internal rooms housing servers, switches, or network equipment must include at a minimum fire suppression, HVAC controls, power loss and prevention, emergency lighting and power,

and environmental monitoring. Cabling must be secured and shielding in place as necessary. As required by local laws and regulations, water damage, earthquake, or other protections must be in place. Critical equipment that cannot meet environmental standards must be relocated to meet these requirements. The Organization *Physical and Environmental Security Policy* provides additional guidance on how we maintain secure facilities globally.

C. System Maintenance
    a. Accountability for equipment and hardware maintenance (servers, switches, other physical equipment managed by Organization) is the responsibility of the designated System Owner in the IT Infrastructure team. We outline system maintenance requirements that System Owners need to follow in the Organization *System Maintenance Policy.*

D. Media Protection
    a. Physical files, documents, hard copy materials, and removable storage media containing Confidential or Highly Confidential Information must be stored, transported, and destroyed in a secure manner. Any procedures for media handling must be in accordance with retention policies established by Legal and Finance. Sanitization or masking may be an option. Contact Information Security for information on masking, sanitization, and disposal methods.
    b. Where appropriate, Organization employees may mark media (documents, tapes, etc.) with its classification category. Marking may be required by applicable laws or directives.
    c. Laptops are tracked and identified by a Service Tag asset identification number maintained by IT. Contact the Service Desk immediately if any laptop is lost or stolen.
    d. Contractors or consultants approved to use their company-provided equipment to conduct Organization business are responsible for physically securing equipment in their possession. Any loss of equipment containing Confidential or Highly Confidential information, even if vendor-owned, must be reported immediately to Information Security. Additional media protection requirements can be found in the Organization *Media Sanitization Policy* and the Organization *Clean Desk Policy.*

E. Mobile Device Protection
    a. Connectivity to Organization networks is permitted from any device, whether Company-issued or personal. Authorized employees use a third-party portal to request and manage company-issued cell phones. Users are responsible for protecting these and other portable devices to avoid the potential security risks to the corporate network. For Company-issued devices, occasional personal use is permitted, but all devices, phone numbers, and the information they contain are the property of Organization and must be returned to the Company prior to leaving the firm. Lost company cell phones must be reported to the Service Desk and the third- party provider for replacement. Lost or stolen devices can be wiped remotely with procedures available from the Service Desk. Additional guidance can be found in both the Organization *Mobile Device Security Policy* and the Organization *Bring Your Own Device Policy.*

V. System Protection

A. Operations controls
    a. Essential operations procedures for equipment, infrastructure, and virtual environments maintained by Organization must be documented. Documentation should cover installation and configuration of systems, processing and handling of automated or manual inputs, backups, scheduling requirements, error handling, key contacts, restart and recovery activities, logging and monitoring, Service Level Agreement (SLA) requirements and any contractually-agreed procedures. Operations procedures should be made available to all users who need them.
    b. Gateways and servers must be configured with a login notification or banner that complies with any applicable laws and regulations. As appropriate for the system's purpose, the notification should indicate that any information system usage may be monitored, recorded, or subject to audit. Systems must use internal system clocks to generate time stamps for synchronization, such as Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).
    c. In addition to the above, systems and applications should be hardened (or optimally protected) appropriately by using InformationSecurity system hardening controls, thus securing systems before they are installed in the production area of the Organization Global Network. Additional system and application hardening guidelines are outlined in the Organization *System Hardening Policy*.

B. Firewalls and Connectivity
    a. Firewalls are in place to control the flow of information and where it is allowed to travel. Connections between the internal network and external networks must be made through approved connection points. Organization systems connected to untrusted networks (i.e. open Internet, vendors, etc.) must be protected by firewall technology. Remote access must utilize an approved access method such as the approved VPN solution.
    b. Firewalls are deployed at each of the Organization's performance hubs globally to restrict inbound and outbound connections to the Organization network from the Internet and other untrusted networks. Dedicated connections between information systems must be carefully considered given the different security requirements and controls that may be implemented on the external system. Requests for authorization of additional connection ports and addresses must be requested by emailing a completed Firewall Policy Change Request form.
    Only Company-approved devices are allowed to connect to Organization resources. Connections originating from unknown devices (e.g., laptops, cell phones, tablets, USB drives, and any other equipment that may connect via device connection ports) are recognized through continuous monitoring of Network Access Control (NAC) software. All equipment connecting to the Organization network, including machines, phones, tablets, cameras, can be tracked by MAC address through firewall software.

C. Applicable Protection
    a. Sensitive systems or applications may be segregated physically or logically to maintain a higher level of protection. Logical security in multiple applications separates functions, teams, and processes in shared resources.

VI. Vulnerability Management

A. Vulnerability and Integrity Management

a. The Organization utilizes a variety of tools in the Threat and Vulnerability Management program. These include asset inventories, regular scanning of assets to identify vulnerabilities, logging and monitoring. Multiple products and utilities are used within IS to identify, track, monitor, and remediate vulnerable systems and software. Flaws are reported and corrected depending based on criticality. Systems or applications managed by the Organization are configured when possible to fail in a known safe state to help prevent failing in a state that could cause a loss of integrity or disruption.

b. Several teams within IS receive information security alerts and advisories from industry sources, professional organizations, and vendors. Potential threats are shared through cross-organization information sharing tools such as the company social media platform.

B. Anti-Virus, Malware, and Spam

a. The Organization employs anti-virus protection software at server and system entry and exit points to detect and eradicate viruses and malware. The software is updated at system startup and when performing various daily actions, sending an alert when malware is detected. Incoming email is inspected, with messages that may contain a virus, spam, or inappropriate content sent to a quarantine area for user disposition. We provide additional requirements for all users in the Organization *Anti-virus Policy*.

C. Software Integrity

a. Systems and tools are in place for checking integrity in systems, software, and applications in production. Appropriate IS or business units are notified as needed with system state notifications regarding startup, restart, shutdown, or abort actions taken by operational systems, or are notified by third parties who may be managing equipment or software. Other checks may include memory protection, input and output validation, error handling, and output filtering.

b. Many Organization applications are platform-independent and employ virtualization, which aids easy deployment of diverse operating systems and applications. These architectures also make it more challenging for an adversary to carry out successful cyber-attacks using advanced persistent threat (APT) methods, by reducing exposure to physical infrastructure through concealment and misdirection. Databases also utilize checks and alerts to determine if atypical database queries of accesses occur that could indicate data mining.

D. System Monitoring

a. Systems that provide initial entry/authentication into the Organization network, remote access gateways, and any application system that processes Confidential or Highly Confidential information must be configured to capture continuous security audit log data. At a minimum, logging should include the identity of the person or process accessing the system, logon success or failure, and login/logoff timestamp. Activities of those with privileged accounts

that have a higher level of access on servers or within applications should be captured and recorded in security audit logs.

b. System or application administrators must routinely monitor system logs for anomalies regarding access, for investigative purposes and to identify patterns that will help predict and prevent failures. Exceptions to security policy must be investigated and appropriate action taken.

c. Logs must be protected from unauthorized modification or destruction by those who are not authorized to access them. Security audit logs should be retained for a minimum of 30 days, or longer as required for compliance, legal reasons, or to support investigations. Review the Organization *System and Information Integrity Policy and Audit and Accountability Policy* for additional requirements.

VII. Networks and Cryptography

A. Network Security

a. The Organization's offices are connected through a high-performance, all-wireless network architecture. Each office is connected to one of the hosted performance hubs that provide firewall and wireless connectivity to the primary cloud environments. The IS Infrastructure team manages firewalls, remote access software, and wireless environments. A third party monitors our wide area network and circuits through their 24-7 Network Operations Center (NOC).

B. Wireless Security

a. The Organization's network environment uses wireless transport for both data and voice communications and transport, integrated with email, collaboration, and business tools. IT Infrastructure is responsible for protection of internal and external wireless communication links that may be visible to individuals who are not authorized system users. Controls are in place to reduce interference and reduce external detection.

b. A Guest wireless network is available. Employees can request and manage temporary accounts through a Guest Provisioning portal. Some conference rooms designed for visitors are configured with a feature allowing temporary access to internal servers via the A/V display.

c. Instructions for company-issued phones to connect to the wireless network are available through Help Desk. Contact the Help Desk if assistance with wireless options is needed, and to review additional requirements, review the Organization *Network Security Policy* and the Organization *Mobile Device Security Policy*.

C. Encryption

a. The Orgaqization requires that encryption be used in compliance with laws, regulations, client directives, or whenever Confidential or Highly Confidential information is stored or transmitted. Encryption must be used in the following situations:

1. When transmitting Highly Confidential or Confidential information through untrusted or external networks.
2. Information classified as Highly Confidential or Confidential, which includes health-related information protected by HIPAA (the Health Insurance Portability and Accountability Act) and personally identifiable data as required by MA 201 CMR 1700.

3. The Organization's laptops must be encrypted. If your laptop is not encrypted, contact Information Security.
4. All passwords must be encrypted and unreadable. This includes password files for users, firewalls, routers, operating systems, applications, databases, and web servers.

b. Cryptographic keys used by websites and products are managed by the IT Infrastructure team. Contact Information Security for all questions regarding encryption, and also review the Organization *Encryption Policy.*

VIII. Systems Development & Change Management

A. Systems and Application Development

a. Systems and applications being designed, developed, or implemented should ensure that the resources needed to implement information security are included in planning and investment processes. Applications developed for our internal use and for client projects must include security considerations at all key stages of the applications development life cycle. Any security requirements mandated by regulatory, contractual, or industry standards must be addressed. Essential security requirements, such as authentication, administration of access rights, secure remote access, and the type (classification) of data being processed should be defined at the beginning of the project.

b. Application managers should consider secure coding practices that will prevent or minimize security vulnerabilities, especially for any Internet-facing applications. If a third party is hosting an application, data protection controls provided by the third party must be adequate to meet regulatory and contractual requirements for security.

c. Program source code should be protected by restricting access to only those with a need-to-know. Version controls for source code should be in place to maintain application integrity. Business Application Owners are responsible for ensuring these and other necessary security controls are in place.

d. Confidential and Highly-Confidential Information or data that is used for testing purposes must be scrambled or masked prior to use. *Please refer to the Organization's Deidentification and Reidentification Policy.*

e. For further guidance on secure system development, review the Organization *Secure Coding Policy*, the Organization *Non-Production Policy* and the Organization *Information Classification Policy*.

B. Change Management

a. Application change control is a security issue because unauthorized or accidental changes to applications may impact the integrity and availability of the data. For this reason, application development activity must be separated from production environments, and access to production must be limited to authorized users. Wherever possible, those who develop code should not also be the same individuals who may change it or access it in a production environment is one example of separation of duties to maintain integrity.

b. Change Control processes are required to mitigate risk associated with modifications to business applications, minimize the impact of change, and to provide a stronger linkage between production

problems and the events that caused them. Some applications managed by IT are controlled through a change and release management process linked to the Help Desk request system. The owners of business applications that are not supported by IT are responsible for establishing and enforcing change control processes for applications they maintain.

c. Employees may download company-approved software via a link on the internal company home page.

IX. System and Services Acquisition

A. System and Services Acquisition Policy

a. The Organization can implement security controls across technology platforms when they are acquired according to Information Security and Purchasing Department guidelines. Application software, IT-related consulting and contracted services, and hardware and systems software must be reviewed by the Information Security team to ensure the proper data security and information protection measures are in place before acquisition. Detailed guidance is in the Organization *System and Services Acquisition Policy*.

X. Security Incident Response

A. Security Incident Response Policy

a. Security incidents ranging from compromised passwords to lost laptops can potentially disrupt business operations as well as exposing sensitive or proprietary information. A breach of categorized (classified) information could have far reaching negative impacts to the Organization's business and reputation. Although standard operating procedures can vary within Organization business areas, a consistent approach to security incident response can minimize the extent and severity of security exposures.

B. Security Incident Response Plan

a. A Security Incident Response Plan details requirements and procedural steps that will enable a quick and effective recovery from unplanned security events. The plan contains requirements for responding to security incidents or breaches, roles and responsibilities, and basic procedures needed to respond in a systematic manner. The plan contains a reporting template, contact information, and additional resources.

C. Security Incident Processes

a. Incident response is an expedited reaction to an issue or occurrence. Those responding must react quickly, minimize damage and restore resources, all the while attempting to guarantee data integrity and preserve evidence. There are four main phases in the process: (i) immediate actions, (ii) investigation, (iii) resolution, and (iv) reporting. Security incidents are categorized by type (Internal, External, Technical, or Physical Loss / Theft) and by impact (Severe, High, Medium, or Low). Incidents that could represent a breach of personally identifiable information may affect laws or contractual commitments. These have a separate set of procedures to ensure proper response.

b. The Help Desk maintains procedures for all types of incidents, including those affecting business-critical processes. These Priority 1 incidents have both a High Urgency and a High Impact rating, demanding a response beyond the routine.

c. Users detecting potential security incidents or incidents of a general nature must immediately report them to the Help Desk, who will notify the appropriate response teams in order to begin investigation and resolution of the incident.

XI. Business Continuity

A. Business Continuity

a. Disaster recovery plans describe how systems and resources will respond to a disaster situation and restore processing to the business, based on the Organization's business objectives and timeframes for recovery of critical applications. IT will provide overall coordination and management in the event of a disaster, and assemble Operations, Network, Facilities, and Communications teams to provide a timely response. Further information is documented in Organization Disaster Recovery Plan and the Organization *Business Continuity Policy*.

b. Business Continuity Plans are departmental plans that describe in detail how the business area will continue functioning in the event of a major system outage or a disaster. Each major business area is responsible for documenting a Business Continuity Plan and designating a Business Recovery Coordinator who will develop and maintain their plan and participate in notification and recovery activities.

B. Backup and Recovery

a. The Organization's data is regularly backed up and copies are kept offsite based on defined business requirements for information recovery. Backup media is sent offsite on a daily and weekly basis and maintained securely by a third-party offsite storage provider. Backup media on the premises must be kept physically secure at all times. Backups may only be requested from the offsite storage provider by authorized staff.

b. Critical information must be stored on network shares to ensure regular and automatic backup and recovery. Critical information must not be stored on personal computers or laptops alone, or on unencrypted personally-owned devices. If additional storage space is needed, contact the Service Desk for options.

c. For applications not managed by IT, the relevant Business Application Owner is responsible for ensuring adequate backup and recovery mechanisms are in place.

XII. Audit and Accountability

A. Audit

a. Audit reviews are conducted by external auditors and consultants on a regular basis. General controls are reviewed by the Organization's corporate external auditor annually. Selected application security reviews may be performed as part of general controls audits. Additional information regarding audit and accountability is contained in the Organization *Audit and Accountability Policy*.

B. Security Assessments

a. Information Security performs periodic testing and audit of systems and applications to ensure correct operation of systems and ensure that security controls are working properly. Information Security performs monthly vulnerability scans that are reviewed by IT system owners. Penetration testing of vulnerabilities noted are performed on

an as-needed basis. Other security assessment requirements are located in the Organization *Security Risk Assessment Policy*.

XIII. Privacy

A. Privacy Management

a. The Corporate Compliance department and Information Security manage the Organization Privacy Program, and monitor potentially relevant statutory, regulatory, and contractual requirements that may affect the company. Many regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), the Massachusetts MA 201 CMR 1700 data protection law, the General Data Protection Regulation (GDPR) and U.S. state security breach notification laws define specific actions to be taken in the event of a security or privacy breach. Processes for response(s) to breaches that may have an impact on individuals' privacy require close collaboration with Information Security.

b. The Organization Privacy Statement is posted on the Organization public web site and maintained by Information Security and Corporate Compliance Office, who also maintain the policy Global Data Protection of Personal Information found in the Organization Employee Handbook.

c. Legislative requirements vary from country to country and may vary for information created in one country that is transmitted to another country. Individual contracts may set out terms for transfers of data internationally.

d. As a result of expanding privacy regulations, Privacy Policies are addressed regionally in each region's employee Handbook.

B. Data and Information Protection

a. The Organization takes steps to guard against unauthorized access to Organization Confidential information maintained by the Organization. Only authorized and approved users with the appropriate level of access to the information that is necessary to accomplish designated responsibilities is allowed. In some cases, we are contractually and/or legally required to implement and maintain certain information security practices. Among those practices is the adequate protection of Information against expected threats that we identify through Information Security threat models.

b. Additionally, Privacy threat models are also used to addressed privacy risk, through either manual or by using a data de-identification tool. As part of the Organization data/information protection strategy, de-identification tools can be used when data/information protection is required. The Organization *De-identification/Re-identification Policy* provides guidance on requirements for protecting Confidential and Highly Confidential Information, including Personally Identifiable Information, when required.

Exception

Requests for exception to this policy must be submitted for approval to ISy@organization.com. If approved exception is only granted for up to 1 year.

References

Organization Information Risk Classification Policy

Enterprise Policy Manual IS, Acceptable Use of Information Technology
Employee Handbook Data Protection of Personal Information
Acceptable Use Policy
Access Control Policy
Anti-virus Policy
Awareness and Training Policy
Audit and Accountability Policy
Bring Your Own Device (BYOD) Policy
Business Continuity Policy
Clean Desk Policy
De-identification/Re-identification Policy
Definitions Policy
Email and Messaging Policy
Media Sanitization Policy
Mobile Device Security Policy
Network Security Policy
Non-Production Policy
Password Policy
Physical and Environmental Security Policy
Secure Coding Policy
Security Risk Assessment Policy
System and Information Integrity Policy
System and Services Policy
System Hardening Policy
System Maintenance Policy