Electric

Information Security Policy.

Please be advised the information in this document is strictly confidential and may only be disclosed to duly authorized individuals.

Revision History

Version #	Revision Date	Revision Description	Author/Title
1.0	May 1, 2017	Initial Cyber Security Document	Chad Pry - Director of Product
2.0	April 23, 2018	Annual Review	Chad Pry - Director of Product
3.0	July 1, 2019	Major Revision	Alexander Foley - CISO
3.1	September 17, 2020	Updates to CFO role and credential use.	Alexander Foley - CISO
3.2	September 20, 2021	Clarifying updates to physical security.	Alexander Foley - CISO

Approvals

Approval Date	Title of Approver	Approver's Signature
10/5/2021	Alexander Foley - CISO	DocuSigned by: C8260C3867E54A2...
10/5/2021	Andrew Lazarus - CFO	DocuSigned by: Andrew Lazarus 7B41815388FB405...

Table of Contents

Overview

The policies documented below are a part of executive management's commitment to and leadership in providing a comprehensive Information Security Management Program. The policies are written to provide guidance for implementation of good security practices and help ensure that organizational risk is appropriately mitigated. Effective security practices are essential to business growth, particularly in light of increased regulatory and industry-specific privacy and data breach concerns.

Executive management endorses these policies and works towards continuous improvement of Information Security within the organization. Management leadership is committed to ensuring that appropriate resources are delegated to implementing these policies and the overall improvement of the Information Security Program. Through their leadership and demonstration of compliance with these policies, they help to ensure the Information Security Management program achieves its expected outcome. They support other business managers in their efforts to improve the effectiveness of the program and related security controls.

Enforcement

The organization expects that all employees, contractors, and vendors with access to data are aware of the Information Security Policies and procedures and comply with them. The organization reserves the right to determine appropriate disciplinary actions against employees who do not comply with any of the Information Security Policies documented below. The actions to be taken will be identified by appropriate Human Resources personnel as well as business management. If the violation in compliance to these policies results in a data breach, punitive action may result in termination as well as future civil litigation.

Scope of Information Security Management System[1]

Objective:

This policy serves to identify the overall scope of all the following Policies, Standards and Procedures. It takes into account the mission of the organization, the various departments and organizations that are directly affected by the Information Security Management System (ISMS), and the various information systems, document management systems and the output of these systems, networks, services and products that are part of the delivery of services as part of the overall mission of the organization.

The ISMS is reviewed annually as part of the overall Risk Management program.

Organizational Mission Statement

We're on a mission to revolutionize IT by making it simple, effortless, & lightning-fast for businesses everywhere.

Scope:

Information Systems and Services Provided

There are a number of information systems and services provided. The organization fulfills its mission statement objective by providing services to internal staff as well as customers. This is provided via multiple SaaS, internally developed platforms and services.

Locations

In general, the locations covered by this statement refer to the organization's physical locations. In addition to these, other physical locations, such as third-party service providers, facilities from which staff members telecommute, or access systems remotely. The locations within the scope of the ISMS include, but are not limited to:

- Headquarters - 408 Broadway, 5th Floor, New York, NY, 10013
- Support Location - Rochester, NY
- Support Location - Bangalore, India
- Cloud IaaS and PaaS Providers
    - AWS (Multiple US-Regions and Availability Zones)
    - Heroku (Multiple US-Regions and Availability Zones)

Network and System Infrastructure

All network connections both physical and virtual to these physical or virtual locations are

[1] "ISO_IEC_27001_2013(En).PDF," n.d., 7-8.

considered in scope.

Organizational Scope

Key organizational units that are in scope are those directly involved in providing the delivery of services and that support the network and systems identified above. These include, but are not necessarily limited to:

- Executive
- Customer Success
- Engineering
- Finance & Operations
- Hardware Lab
- Implementation
- Product
- Project Management
- Service Desk, Service Desk - Bangalore
- Service Desk - Rochester
- Workplace (includes Internal IT)
- Marketing

Members of these units under the guidance of the CISO are responsible for insight and update of the scope of the ISMS. Other subject matter experts may also be assigned to provide updates and review of the ISMS.

All organization staff members are responsible for ensuring the practice of good Information Security and are covered within the organizational scope.

Scope Exclusions

There are scope exclusions related to this policy. Exclusions are listed below:

Client networks, operations and systems are not in scope. Electric will implement default, recommended and customer directed security controls and Electric may provide security guidance in support of customers' internal security programs. Customers are responsible for their own internal security policies, standards and procedures outside of the documented Electric scope of services and implemented controls.

Electric is not responsible for client user accounts, with the exception of the secure delivery of requested user accounts and system administration accounts used by Electric for the management of client networks.

Internal References Documents

None

External References

ISO/IEC 27001:Information technology — Security techniques — Information security management systems — Requirements. Geneva, Switzerland: ISO (The Organization of International Standards), 2013.

Management Endorsement

Objective

To provide management direction and support for Information Security, as part of business requirements and in accordance with relevant laws, regulations and industry standards.

Policy

Management is responsible for governance and oversight of the enterprise Information Security Program. They analyze and manage institutional risk; review and recommend policies, procedures and standards; and ensure consistency in disciplinary processes for violation of adherence to policies.

The Information Security Policy is approved by management and supports business objectives and strategy. It is regularly reviewed to ensure that it remains relevant and considers the following:

- ➢ Business strategy and changes in direction
- ➢ On-going legislation, regulations and contracts
- ➢ Current and projected information security threat environment

The Chief Executive Officer (CEO) in conjunction with Board members have assigned general and specific roles and responsibilities for information security within the organization. These roles are granted specific authority and management support in defining information security objectives and principles within the organization. They include the following:

CEO - Chief Executive Officer

The CEO is the highest level executive of the organization and is generally appointed by the Board of Directors. The CEO, along with the Board have complete oversight of the ISMS. The CEO is ultimately responsible for the ISMS program and ensures that:

- ➢ the ISMS program is adequately funded and managed
- ➢ information security risk and mitigating controls are considered at all levels of the organization
- ➢ support for and adherence to the information security program is visible at all levels of management

CFO - Chief Financial Officer

The chief financial officer (CFO) is a senior executive tasked with overseeing the day-to-day administrative and operational functions of the business. The CFO typically reports directly to the chief executive officer (CFO) and is considered to be second in the chain of command.

This individual is responsible for liaising with the CEO and other C-level executives to ensure that:

- overall operations support the Information Security Management program
- technology initiatives have been thoroughly reviewed
- business operations are appropriately considered as part of information security planning
- business impact related to disaster recovery and business continuity is accurately reported and assessed
- ensuring that key performance indicators (KPI) related to the overall operations as well as information security program indicators are captured and accurately reported

CTO - Chief Technology Officer

The Chief Technology Officer is responsible for the overall technical direction of the organization and ensures that the technology that is adopted supports business objectives and goals. In addition, the CTO is responsible for ensuring that technology is appropriately tested, securely implemented, and addresses the needs of the business. All technology initiatives must be formally reviewed and approved by the CTO. This role is functionally held by the SVP of Engineering.

CISO - Chief Information Security Officer

This role is responsible for overall security in the organization. The CISO works in conjunction with the CTO to ensure that security concerns and requirements are addressed, and that the information security threat environment is reduced or remains stable as a result of new technology. This role is responsible for the review of the overall risk management program. The CISO is responsible for:

- Developing appropriate policies and procedures to comply with applicable regulations and standards.
- Overseeing the security of data.
- Monitoring compliance with the company's security policies and procedures through review of internal audits and assessments.
- Identifying and evaluating threats to the confidentiality and integrity of data.
- Responding to actual or suspected breaches in the confidentiality or integrity of data.

All major initiatives that involve the development or acquisition of software, implementation of infrastructure, etc.that processes, stores or transmits sensitive or regulated data must be formally reviewed and approved by the CISO.

Compliance/Privacy Officer

This role is responsible for ensuring that all industry standards, and state and federal regulations related to data being processed, are being met by the organization on an ongoing basis. The Compliance/Privacy Officer is responsible for the development and implementation of the policies and procedures required to comply with Data Privacy Rules as defined by various regulatory bodies. This role is functionally held by the CFO.

This role is also responsible for:

- ➢ Understanding the Data Privacy Rules and their applicability to the organization.
- ➢ Overseeing the enforcement of client privacy rights.
- ➢ Monitoring compliance with privacy policies and procedures.
- ➢ Developing and ensuring employee training process is in place.
- ➢ Notifying the CISO of any Business Associate Agreements, PCI Requirements or other state or federal privacy regulations that may apply which affect regulated data, prior to the execution or amendment of any such agreement.
- ➢ Receiving and responding to complaints of alleged non-compliance with Data Privacy Rules.

The Compliance/Privacy officer liaises with the CISO and provides guidance as to the security requirements for handling sensitive or regulated data through its lifecycle. Internal audit and management of external audits and assessment, are the responsibility of the Compliance/Privacy Officer.

Executive management endorses the creation of appropriate policies and processes as well as specific processes for handling deviations and exceptions. They also ensure that Information Security management is integrated into the organization's overall processes. Executive management ensures that the need for effective information security is communicated to the organization and that appropriate resources are available for the implementation of such security.

Finally, executive management promotes continual improvement and supports other relevant management roles to demonstrate their leadership, as applied to their areas of responsibility.

Internal Reference Documents

None

External References

ISO/IEC 27001:2013, 2nd Ed. Section 5.1 Leadership and Commitment; Section 5.3 Organizational Roles Responsibilities and Authorities.

ISO/IEC 27002:2013, 2nd Ed. Section 5.1 Management Direction for Information Security; Section 6.1.1 Information Security Roles and Responsibilities.

Risk Management

Objective

To implement a risk management program where information security risk assessment is part of ongoing operations in order to ensure risk is appropriately assessed and remediated.

Policy

Risk management is dynamic and designed to adapt to the organization's developments and changes to the risk profile over time. Ongoing risk assessments are made as part of the Information Security Management Program and are repeated at regular intervals, and when major changes to the business organization, infrastructure or technology direction are made.

The organization's risk management program is based on a structured and systematic process that regularly evaluates the organization's internal and external risks. The main elements of the risk management process are as follows:

- **Communicate and consult** – The CISO is responsible for initiating the risk assessment process. The risk assessment is completed by appropriately trained staff or external parties. The CISO also communicates and consults with internal and external stakeholders as appropriate at each stage of the risk management process and concerning the process as a whole.
- **Establish the context** – Executive Management is responsible for establishing the overall context for the risk management process, such as the criteria against which risks are evaluated, the business and regulatory context, the structure and format of the analysis is defined.
- **Identify risks** – The organization or staff responsible for performing the risk assessment, identify where, when, why and how these risks may prevent, degrade, delay or enhance the achievement of the organization's objectives.
- **Record risks** – The organization or staff performing the risk assessments provides interim and final documentation of all risks that are identified as part of the assessment.

- **Analyze and evaluate risks** –The CISO, in conjunction with other executive management analyzes consequences and the likelihood of the documented risk by examining the potential consequences and their impact upon the organization. This evaluation compares the level of identified risk against the organizational risk profile. This enables decisions to be made about the extent and nature of risk treatment required.

- **Threat risks** – Executive management is responsible for evaluating existing controls and treating excessive risk identified as part of the risk assessment. This process includes developing and implementing strategies for treating this risk by identifying and evaluating existing controls. Develop and implement specific cost-effective strategies and a treatment plan for improving effectiveness of existing controls and implementing new controls to increase organizational benefits and reduce risk profile. The CISO is responsible for ensuring that the treatment of risk, development of new controls or improvement of existing controls is appropriately implemented.

- **Monitor and review** –The completed assessment will be presented to executive management for review and analysis. Management is responsible for monitoring the overall effectiveness of the risk management process. This process is crucial so that changes in the organization's business direction do not alter priorities. Regular internal and external risk assessments are used as part of the overall risk management process and are scheduled as needed to ensure compliance with industry standards, federal and state regulatory requirements.

Audit and Assessment

Both internal and external audits and assessments are essential to ensuring that the information security risk management program remains effective and meets performance improvement expectations.

1. The audit process includes review of various operational and security control activities and processes. These include, but are not limited to:

    - Review of application, network, server and system configuration standards and adherence to these by IT Operations staff
    - Review of security administration and access controls as evidenced by access review, documentation of user additions, modifications and deletions
    - Review of other monitoring and risk management controls, such as vulnerability assessment and penetration testing results

2. The Compliance/Privacy Officer or designee is responsible for the ongoing internal review and assessment process in the absence of an Internal Audit function. This process includes:

    - Establishing appropriate intervals for assessment

- ➢ Establishing assessment and testing process
- ➢ Communicating to departments being audited
- ➢ Requesting and gathering documentation, and ensuring that such information has not been altered
- ➢ Performing testing according to stated testing process
- ➢ Delivering results to CISO and executive management
- ➢ Review compliance and effectiveness of control environment

3. The Compliance/Privacy Officer is responsible for managing external, third-party assessments or audits as needed. Such audits may be performed by clients, business associates in execution of their Vendor Management program, or when the organization is financially material to a publicly traded company, etc. The process includes, but is not limited to:

    - ➢ Coordinating scheduling of third-party auditors
    - ➢ Responding to documentation requests
    - ➢ Facilitating audit process by assisting with interviews, process walk-through, clarifying questions, etc.
    - ➢ Ensuring that audit results are accurately represented
    - ➢ Assisting with management responses to audit report
    - ➢ Preparation of remediation plan in conjunction with CISO, CTO, CFO and IT Operations
    - ➢ Oversight of remediation
    - ➢ Update of internal assessment and control processes

4. Executive management is responsible for management responses to external audits and for the review of internal review and assessment reports.
5. All results of audits and assessments, as well as resulting test artifacts, are retained as part of the risk management and audit process.

Internal Reference Documents

Risk Management Standards and Procedures

External References

ISO/IEC 27001:2013, 2nd Ed. Section 6.1.2 Information Security Risk Assessment.

NIST Special Publication 800-30, “Guide for Conducting Risk Assessments.” Sept. 2012: Chapter 2, Section 2.1 The Risk Assessment Process.

ISO/IEC 27002:2013, 2nd Ed. Section 6 Organization of Information Security.

Data Classification

Objective

To identify the level of protection required for information assets, based on the level of risk to the organization if data is accessed in an unauthorized manner or compromised.

Policy

Data must be protected from unauthorized access and compromise or disclosure. Data must be appropriately categorized to ensure that it is handled concomitant with the level of risk. The organization has adopted this data classification policy to help manage and protect its information assets.

1. Information must be protected based on its level of classification. Where information is grouped together, the highest classification is applied to all information in the group and must be protected based on this classification.

2. Business owners are responsible for identifying data for which they are responsible.

3. Data classification inventory is reviewed and updated periodically. The CISO reviews and approves classifications of sensitive or regulated data.

4. All data at the organization shall be assigned one of the following classifications:

   Public - Information that can be made available in the public domain and which would not cause damage or harm if released.

   Internal Use - Information generally available to anyone within the organization and which contains business value to the organization.

   Confidential - Information the unauthorized disclosure of which (even within the organization) would cause serious damage in terms of financial loss, legal action or loss of reputation.

   Sensitive/Regulated - This is data that contains non-public information such as bank account information, PHI (Private Health Information), Social Security Numbers, and other such information that has been identified in state and federal regulations as sensitive. It may also include information that is generally understood to be sensitive due to its use as an account identifier (e.g., an email account used as a login user name).

Internal Reference Documents

Data Classification Standards and Procedures

External References

ISO/IEC 27002:2013, 2nd Ed. Section 8.2 Information Classification; Section 8.2.1 Classification of Assets; Section 8.2.2 Labelling of Assets.

Data Management

Objective

To ensure that all data is handled appropriately with reference to its data classification and importance to the organization at all stages of its life cycle. Data management must ensure that appropriate confidentiality, integrity and availability is maintained; and must be compliant with all applicable federal and/or state laws.

Policy

The protection of data is a critical business requirement; protection methods must remain flexible so that data may be accessed by authorized individuals, and staff may effectively perform their job functions. Any information system that stores, processes or transmits data for which the organization is responsible, must be secured in a manner that is considered reasonable, appropriate, and compliant with well-known information security standards, federal and/or state Laws, and contractual requirements.

Data Capture

Data within the organization may be captured using a variety of methods. Those most often used are: Data Entry (end-user generated), Data Acquisition (purchased or integration), and System-Generated.

Data Entry

Typically data is entered into an application, form or web-page. Such data entry will be protected as follows:

Public Information - The data entered over an unsecured network, such as the public internet, should be scanned for malicious code, scripts, etc. Otherwise, no further protection of such data is required.

Internal Use - This data must be entered over a secured network, either on an internal network, using a VPN (Virtual Private Network) connection, or an otherwise secured site. Such information may not be made available to unauthorized individuals or persons external to the organization.

Confidential - This data will be masked as appropriate; for example, accounting information, personnel records, etc. The entry point for this data will be flagged with the label of "**Confidential**" to ensure that the end-user entering the data is aware of the sensitivity level of the data.

Sensitive/Regulated - All data that is sensitive or regulated in nature must be entered over an appropriately secured network. This includes the use of TLS, VPN technology, etc. In addition, this data must be masked during entry and subsequent display of the data must be truncated to conform to industry, federal and/or state regulations. For example, a Social Security Number may not display more than the last four digits.

Data Acquisition

All data sources / categories of data that are acquired by the organization must be reviewed by the Compliance/Privacy Officer and/or the CISO to determine the appropriate data classification. Based on this review, this data is labeled, and data classified as **Confidential, Sensitive** or **Regulated** is secured through the use of strong access controls and encryption, tokenization, masking, etc. as appropriate.

Data that is classified as **Internal Use or higher**, is so labeled, and distribution to external or unauthorized parties is disallowed.

System-Generated

Data that is created or modified in some way through the processing of an information system is classified and labeled as part of the creation or modification process. This processing can include the calculation of new values, and appending two or more non-sensitive data fields to create a new field that increases the data classification of the new record. For example, appending the month, day, year and age fields to create a new datum field would change the classification of the newly created field to Sensitive/Regulated (HIPAA). **Confidential, Sensitive** or **Regulated** data created through the action of an information system is secured through the use of access controls, encryption, etc.

Data that is classified as **Internal Use or higher**, is so labeled and further processing is restricted to internal systems.

Data Processing and Storage

Data processing is defined as "the converting of raw data to machine-readable form and its subsequent processing (such as storing, updating, rearranging, or printing out) by a computer." [2] This includes a variety of activities such as the input, transmission, and calculation of new values through the actions of an application, the output of data in a variety of formats, etc.

[2] "Data Processing | Definition of Data Processing by Merriam-Webster." 20 Oct. 2017, https://www.merriam-webster.com/dictionary/data%20processing.

Storage refers to the retaining of data in any format, either electronic or hard copy. This includes all electronic media, such as hard disk, removable media, optical disk, archival media, etc.as well as any hard copy forms, such as faxes or reports printed for distribution by the organization.

1. All processing of this data must be in accordance with its data classification. If ongoing processing of data changes its classification to one that is more secure, the new classification must be enforced. When the data classification is changed to a less secure one, the business owner or data custodian is required to make the determination whether or not to enforce security at the lesser classification.

2. Hard copy data that is being sent to an external source must be securely sent, with measures appropriate to its data classification taken, in order to ensure that the data is monitored and secured from point of departure to point of final destination. Documentation of receipt at final destination is retained by the organization.

3. Data maintained in hard copy form must be stored in a manner that is consistent with the data classification level, using methods approved by the organization. Sensitive and proprietary data must be secured immediately after use and should not be left in public view. Such storage may include secured cabinets, appropriate video monitoring, and restricted access to areas where such data is stored.

4. Data that is digitally stored must be kept in accordance with its data classification level. Sensitive, regulated data must be stored using appropriate security as approved by the organization. This may include encryption, tokenization, restricted access control, etc.

5. All processing and storage of data must ensure the confidentiality, integrity and availability of data concomitant with its classification. Such processing and storage must be maintained throughout the data's life cycle through to destruction.

Data Retention

1. All data and records, both electronic and hardcopy, are retained in accordance with regulatory requirements, compliance with other industry standards, and contractual requirements. A data/record retention schedule is created that considers:

    - ➢ The type of record or data being retained (i.e., internal accounting, database or transactional records, client-provided, operational logging, etc.).
    - ➢ Determination of the appropriate retention period
    - ➢ Contractual and regulatory requirements for data retention
    - ➢ Data classification level

2. All data is assigned to an appropriate retention schedule by the business owner or data custodian in accordance with organization or business needs, and regulatory or

contractual compliance requirements. This includes both live and archival storage of data.

3. Consideration is given to the methods of electronic storage, ensuring that data is accessible throughout the required retention period. This includes the media used for storage, encryption methods, and maintenance of encryption keys throughout the retention period of data.

4. An inventory is kept of all data stored in electronic or hard copy format. This inventory is updated annually and data is cross-referenced, purged and/or the retention period is updated in the inventory.

Data Destruction and Disposal

Failure to properly purge data in a manner that renders the data unrecoverable may pose a significant risk to the company since data often easily can be recovered with readily available tools.

1. All electronic data that is classified as other than **Public** must be reliably erased or the media made completely unreadable using industry standard procedures before disposal.

2. Sensitive or regulated data located on any electronic media must undergo more complete erasure methods. Such procedures may include degaussing, media sanitization as identified in NIST SP 800-88, physical destruction of the media so that it cannot be rebuilt, etc.

3. Evidence that all sensitive/regulated data has been appropriately purged is maintained based on regulatory or compliance requirements.

4. Proof of purging must attest to the erasure of licensed software and company data to complete the disposal or repurposing of company devices.

Internal Reference Documents

Data Management Standards and Procedures

External References

NIST Special Publication 800-53, “Security and Privacy Controls for Information Systems and Organizations.” Draft Rev. 5, August 2017: Chapter 3, Section 3.10-3.12 inclusive.

ISO/IEC 27002:2013, 2nd Ed. Section 8.3 Media Handling

NIST Special Publication 800-88, “Guidelines for Media Sanitization.” Rev 1, December 2014: Chapter 2, Section 2.1-2.6 inclusive

Data Backup and Restore

Objective

To protect against loss of data and to ensure that backup data is restored reliably and timely.

Policy

1. Where appropriate and reasonable, all business data should be stored on SaaS platform providers that provide geo redundant backups as part of the service.
2. For data that is not backed up by a Saas provider:
    a. Data backups occur on a regular schedule, based on the criticality of the data, frequency of update, etc. The schedule is defined based on compliance requirements, contractual obligations, etc.
    b. The extent of the backup (full or differential) and the frequency is based on the business requirements of the organization, and the security and retention requirements of the data.
    c. Backups of data that is considered sensitive, confidential and/or regulated will be secured in a manner appropriate to its data classification. Such backups should be kept in an encrypted state, additionally encrypted in the backup process or at a minimum, password protected. Access to these backups should be restricted in a manner similar to access to the live data and have additional approval and review.
    d. Backups are stored in a remote location or in a facility that is sufficiently distant to escape disaster at the main processing facility.
    e. Backup operations are monitored for successful completion and all issues are addressed such that no data loss occurs.
    f. Backup media should be regularly tested (this may be systematically tested by the IaaS provider).
    g. Data recovery should be regularly tested as well as the procedures to gain access to sensitive, confidential or regulated data.
    h. There is a regular review of backup scheduling and arrangements to ensure that they meet business requirements, including those related to business continuity planning.

Internal Reference Documents

Data Backup and Restore Standards and Procedures

External References

ISO/IEC 27001:2013, 2nd Ed. Section 8.1 Operational Planning and Control.

ISO/IEC 27002:2013, 2nd Ed. Section 12.3 Information Backup.

Asset Management

Objective

To identify the organization's assets and define appropriate ownership and protection responsibilities throughout the lifecycle of the asset.

Policy

1. The organization identifies all assets associated with information and information processing facilities that are relevant in the lifecycle of information and documents their importance. The lifecycle of the asset includes the creation, processing, storage, transmission, transfer, deletion and destruction of the asset.
2. All assets are assigned an **Asset Owner** upon creation or acquisition. Asset owners are considered to be individuals or groups that have approved management responsibility for the asset lifecycle. An asset owner may delegate responsibility for routine tasks, asset maintenance, update, etc., but retains ownership and responsibility for the asset.
3. An inventory of these assets is created and maintained. For the purposes of this policy, assets include but are not limited to:
    a. physical IT assets such as servers
    b. network infrastructure devices,
    c. desktop computers
    d. laptops
    e. mobile devices such as tablets or SmartPhones, purchased by the organization
    f. It also includes logical IT assets such as purchased software, licensing of software, and internally developed applications, Data as an asset has been addressed in the **Data Classification** and **Data Management** Policies.

4. A complex information system[3] that consists of multiple systems, networks, and applications are grouped together and treated as a single information system asset. Individual devices, information assets, etc. will be identified as sub-systems of the overall information system asset.

5. The asset inventory contains all relevant information, and is accurate, up-to-date, consistent and aligned with other inventories. The inventory contains sufficient information to understand the asset's overall importance to the organization, and its value and effective measures to manage associated risk. Such information includes but is not limited to:

    - Assigned asset owner
    - Asset identification as applicable to include:
        - Type of asset (ie., data, software, licensing, hardware, etc.)
        - Description of asset
        - ID or serial number if pertinent
        - Make or manufacturer, and model
    - Location, physical or logical of the asset
    - Data classification of each asset
    - Relationships and dependencies between physical and logical assets
    - Specific security processes or controls (including access controls, backups, etc.) associated with the asset
    - If data classification is identified as **Internal**, **Confidential**, or **Sensitive/Regulated**, the specific type of information being processed, stored or transmitted by the asset should be identified; including but not limited to, intellectual property, sensitive internal information and sensitive/regulated data such as PII[4], PHI,[5] etc.

6. The **Asset Owner** is responsible for ensuring that the asset is correctly classified and all relevant information associated with the asset is complete and included in the organization inventory.

7. The organization conducts a physical audit of IT assets periodically based on compliance requirements ally and this is reconciled to the asset inventory. The organization identifies and resolves e discrepancies between the audit and actual asset inventory.

8. The CTO or CFO, in conjunction with the Compliance/Privacy Officer, is responsible for the maintenance of the asset inventory as assets are acquired and/or removed

[3] "Information system - Wikipedia." https://en.wikipedia.org/wiki/Information_system.
[4] "What is personally identifiable information (PII)? - Definition from ...."
http://searchfinancialsecurity.techtarget.com/definition/personally-identifiable-information.
[5] "Protected health information - Wikipedia." https://en.wikipedia.org/wiki/Protected_health_information.

throughout the asset lifecycle. They, in addition with the relevant asset owners, review and approve the asset inventory reconciliation.

Asset Acquisition

1. All requests for assets must have appropriate approvals by the organization prior to acquisition. The requesting business group must ensure that the review is coordinated with the CTO or CFO who will coordinate with appropriate IT Organizations and groups for review.

2. Software or hardware assets must be verified to be secure and compatible with the organization's existing information systems standards and technical specifications by the CTO or CFO who will coordinate with appropriate IT Organizations and groups for review. prior to acquisition.

3. All assets to be acquired by the organization, other than information assets, [6] are reviewed by the CTO or CFO to ensure that the acquisition is based on consideration of whether the asset:

    - ➢ Provides significant, direct and tangible benefit to the organization.
    - ➢ Is appropriate and cost effective throughout its lifecycle.
    - ➢ Is not duplicative in nature (i.e., it does not exist or an existing asset cannot be upgraded or adapted to meet the same purpose).
    - ➢ Is compatible with existing systems and processes.
    - ➢ Does not increase the overall information security threat environment for the organization.

Asset Planning and Implementation

1. The CTO or CFO and IT Operations are consulted during any major modification to existing information system assets as well as during preparation for the acquisition of new assets with relation to the following:

    - ➢ Capacity requirements, based on historical trend analysis, and future business and organizational expectations for the asset
    - ➢ Resource availability and training requirements for new assets
    - ➢ Technology compatibility
    - ➢ Infrastructure changes required for new asset
    - ➢ A subject matter expert from the IT Operations team is involved in the planning and overall project management of asset implementation

2. All hardware and software identified as an asset will be appropriately licensed and installed as per manufacturer recommendations to ensure that all necessary security options have been enabled.

[6] See Data Classification and Data Management Policies for information acquisition.

3. The CISO and CTO will review implementation procedures to ensure that they are complete, and consider the security and stability of the organization's environment.

4. All asset implementation will follow Change Management Policy..

Internal Reference Documents

Asset Management Standards and Procedures

External References

ISO/IEC 27002:2013, 2nd Ed. Section 8 Asset Management: Section 8.1-8.1.2 inclusive.

Vendor Management

Objective

To ensure protection of the organization's data assets that are accessible and/or processed by vendors (suppliers).

Policy

1. All vendors are reviewed and classified with reference to the types of information assets or services that the vendor is storing or processing. All vendors are identified and documented as to the type of services provided. A security risk profile (low, medium, high risk) and business impact profile is initially assigned to each vendor and is based on the sensitivity of the information being processed or the criticality of the vendor to the business. This is regularly reviewed for applicability.

2. There is a standardized process and life cycle for managing vendor relationships. This includes the acquisition, review, management of contracts, and documentation of responsibilities of the vendor to the organization.

3. The type of information access to the organization's internal systems will be defined, as well as the monitoring and controlling of said access.

4. Minimum information security requirements are defined for each type of data that is consistent with the organization's data classification standards and serves as the basis for individual supplier agreements. This includes the following:

    - Handling of incidents and contingency planning as needed
    - Resilience and recovery to ensure availability of information or information processing provided by the vendor

- ➢ Awareness training for the organization's personnel regarding applicable policies, processes and procedures for handling data and interacting with vendor personnel
- ➢ Awareness training for the vendor organization as required based on the type of services provided by the vendor and the level of access to organization data, as well as the data classification of the information accessed
- ➢ Training for the vendor organization in handling external parties, such as organization customers/clients as appropriate

5. Vendors who have access to sensitive, confidential or regulated data are classified as having a higher risk profile and therefore will require the following:
   - ➢ Information security requirements clearly documented and agreed upon
   - ➢ An initial security review; all items determined by the CISO or designee of medium or high risk must be remediated prior to use by the vendor. The CISO or designee may approve the use of a vendor prior to remediation with a documented plan for remediation in place and alternate compensating controls.

6. A complete record of all vendors and related contracts is maintained by the CFO (designee.) Ongoing performance metrics and information security review results are included in this record.

Contract Management

Contracts or Terms and Conditions define the roles and responsibilities of each party in the contract and documents expectations for the relationship. Minimum contract requirements are documented below as related to contract management. They provide a baseline of requirements that may need to be expanded for vendors providing critical services or processing, storing and/or transmitting sensitive, confidential or regulated data.

All vendor agreements are initiated by business management and submitted for review by appropriate groups, that include Financial Management and may include IT Management, the CISO or designee as appropriate.

1. Contracts are reviewed with respect to the following:
   - ➢ Processes and procedures for monitoring adherence to established information security requirements.
   - ➢ Vendor management of data processing and information assets.
   - ➢ Scheduling of software and/or system updates is included, depending on the services provided.
   - ➢ Service up-time and penalties based on the business requirements and risk exposure due to downtime.
   - ➢ Handling incidents and responsibilities of both parties.

2. Transition, transfer or other movement of information, information processing facilities and anything else requiring movement during transition to or from vendor services must

be specified, including provisions for maintaining appropriate information security relative to data classification.

3. Contractual obligations for the maintenance of agreed upon security and the right to audit as appropriate.

4. Legal and regulatory requirements of information processing and how vendors will meet said requirements should be itemized as appropriate.

5. Vendors providing consulting or other contracted services, such as software development and staff augmentation services will have employment requirements at least as stringent as the organization. Vendor staff members must be:

   - ➢ Appropriately vetted as part of the on-boarding process at the vendor organization.
   - ➢ Vetted and reviewed by the vendor organization as needed, including but not limited to a background check.
   - ➢ Required to work on a secured and approved computer or virtual computer image.
   - ➢ Not allowed access to sensitive data unless specifically approved by business owner and CISO or designee.

6. Depending on the service provided (i.e., application development, IaaS), Non-Disclosure Agreement (NDA) considerations should be included. Ownership and copyright of code developed by the vendor on behalf of the organization should be detailed.

Vendor Reviews and Assessment

Vendor review and assessment is a key component of vendor management. Such review is done to ensure performance objectives are being met and to ensure that the organization's information assets, processing facilities, administration, etc. are being processed with the agreed upon level of information security based on the risk profile of the vendor.

1. Vendor reviews occur on a regular, timely basis depending on the risk profile of the vendor.

2. Information security reviews are performed and managed by the CISO or designee.

3. Performance reviews are initiated and managed by the business manager of the vendor relationship. This should occur at a minimum on contract renewal, or more frequently as needed.

4. Gaps in performance or in maintenance of information security requirements must be reviewed and a remediation plan developed and implemented. Further reviews to ensure remediation has been completed may be done.

5. The Business Manager and/or the CISO (designee) must review and approve the results of the assessment.

6. Depending on the vendor contractual requirements, the contract may be terminated based upon a negative review.

Business Associates Agreements

In addition to aforementioned contracts, vendors who process, store, transmit or provide services that affect sensitive, confidential or regulated data are required to sign separate business associate agreements in compliance with specific industry standards and/or federal or state regulations. These agreements shall be renewed on a regular schedule and vendors are subject to review of the terms of the agreement.

Internal Reference Documents

Vendor Management Standards and Procedures

External References

ISO/IEC 27002:2013, 2nd Ed. Section 15 Supplier Relationships: Section 15.1-15.2 inclusive.

Workforce Security

Objective

To ensure that the organization's workforce understands their responsibilities and are suited for their roles, and to define roles and responsibilities to ensure that they are appropriately segregated in order to reduce opportunities for collusion and fraud.

Policy

For the purposes of this policy, workforce is interpreted as all directly hired employees, either full-time or part-time, contractors and consultants, or other service providers that have been appropriately reviewed as part of Vendor Management (See Vendor Management Policy.)

Onboarding (New Hires)

1. All potential workforce positions must be requested and individuals identified by appropriate business management via the HR onboarding procedure.

2. All positions will have job duties clearly specified and documented, particularly information security requirements. All job descriptions will include the minimum level of education, certification and experience required to be considered for hire.

3. All potential staff members must have sufficient background checks to ensure that they are suitable for the roles for which they are being considered.

4. Verification of their suitability may include the following as appropriate:

    - ➢ Availability of satisfactory character references.
    - ➢ Independent identity verification as required by local, state and/or federal regulations which will include use of federal or state approved identification verification such as a passport, license and/or presentation of Social Security number (SSN.)
    - ➢ Credit or criminal review as applicable.

6. Where potential staff members will have root, administrative or other privileged access to sensitive data, onboarding verification checks require criminal record review.

7. The organization ensures that all potential workforce members have the necessary experience and competence to perform their job functions and can be trusted to assume the role, especially if it is critical to the organization.

8. Management identifies criteria to determine disqualification based on verification of background. These are documented.

9. All verification must be completed prior to granting any access to company data to the workforce member, unless explicitly waived by the CISO or designee. Falsification or insufficiency of the verification process are grounds for immediate termination.

10. All access must be approved and authorized by the HR Team requesting the potential workforce member. Such requests:

    - ➢ Must be documented as to need, expected starting date and if known, end date.
    - ➢ Must have formal job functions and titles documented.
    - ➢ Roles and responsibilities with relation to confidential, sensitive or regulated data must be explicitly identified.
    - ➢ Must identify the minimum level of access being requested as required for job performance.

9. All workforce members must formally acknowledge their responsibilities for the organization's Information Security Policy by signing a document indicating their understanding .

10. All workforce members with root or administrative access, or access to privileged data, are required to sign a confidentiality or nondisclosure agreement prior to obtaining access to sensitive systems. Failure to do so is grounds for not hiring or terminating an existing employee.

11. Workforce members who are not direct employees of the organization are required to complete a screening process as identified in contractual agreements with the vendor organization.

12. Any screening process that is not completed or does not meet the satisfaction of the organization is cause for termination of the workforce member..

13. All information on candidates for employment within the organization is handled in accordance with appropriate legislation.

Ongoing Employment Security

1. Internal transfers between business groups or departments must be approved by both managers, exiting and receiving.

2. If access to privileged information increases and/or administrative access is required, verification of criminal records review must be completed, if not previously done.

3. All access must be reviewed and access that is no longer required for new job duties must be revoked.

4. All workforce members with administrative or privileged access will accept additional required review and screening.

Disciplinary Process

1. Management has established a formal and communicated disciplinary process to take action against staff members who have committed an information security breach or have abrogated their information security responsibilities.

2. Such action takes place only upon verification that such a breach has taken place.

3. The disciplinary process ensures fair and correct treatment for employees who are suspected of committing breaches of information security.

4. The process provides for a graduated response that takes into consideration factors including:

    - ➢ The nature and gravity of the breach.
    - ➢ The impact on business.
    - ➢ Whether this is a first or repeat offense.
    - ➢ Whether the violator was properly trained in information security responsibilities, relevant legislation, contractual requirements and other factors.

5. Deliberate breaches may require immediate action to be taken; this is done with business management and CISO review and approval.
6. The organization will record all disciplinary actions taken in the employment records of the violating staff member and kept in Company's standard format of Performance Logs.
7. The organization will investigate all privacy and security incidents or violations, and mitigate to the extent possible, any negative effects that the incident may have had, in a timely manner.
8. Neither management nor staff will intimidate or retaliate against any workforce member or other individual reporting a security breach or violation of privacy regulations.

Offboarding (Separation/Termination)

1. The organization will ensure that all access to information assets is terminated upon voluntary separation or termination of a workforce member and when access to those assets is no longer appropriate.
2. Where access to information assets is allowed after separation, specific authorization and approval for access to these assets is documented in a separation agreement and additional confidentiality or non-disclosure agreements (NDA) may be required.
3. The business manager is responsible for ensuring that the appropriate security personnel are notified that access is to be removed.
4. Documentation of removal of access is maintained as required for compliance to applicable standards and for evidentiary purposes.
5. The business manager is responsible for recovery of all physical forms of access granted or assigned to the staff member. Such access includes, but is not limited to, keys, access tokens, identification badges, etc.
6. Any electronic equipment (such as tablets, cell phones, laptops, etc.) owned by the organization, is recovered.
7. Administrative accounts or service accounts are changed timely in the event that separated or terminated staff members are in possession of such access information.
8. Security administration and the business manager are responsible for ensuring that access is disabled and that this is appropriately evidenced and reviewed.

Internal Reference Documents

Workforce Security Standards and Procedures

External References

ISO/IEC 27001:2013, 2nd Ed. Section 7 Support: 7.2 Competence; 7.3 Awareness.

ISO/IEC 27002:2013, 2nd Ed. Section 7 Human Resource Security: Section 7.1-7.2.1 inclusive; Section 7.2.3-7.3.1 inclusive.

Information Security Awareness and Training

Objective

To ensure that all employees, contractors and as applicable third-party vendors receive appropriate security awareness education and training, as well as regular updates in policies and procedures as relevant to their job function.

Policy

1. All employees are trained on the relevance and importance of their activities and how they contribute to the achievement of the organization's policies and objectives.
2. The organization provides sufficient training to ensure that all employees within the organization are adequately trained to enable them to perform their assigned duties. This training will include but is not limited to:
    a. Foundational Security: Confidentiality, Integrity, and Availability
    b. Data Privacy and Compliance with Regulatory and Legal Requirements
    c. Security Awareness, Phishing and Social Engineering
    d. Acceptable Use of Information Assets
    e. Safeguarding Sensitive Information
3. Additional specialized training may be conducted by the staff, including:
    a. Secure Application Development
    b. Secure Administration
4. Individual staff members may need to maintain third party certifications for their role.
5. Mandatory security and regulatory training is provided within the organization to ensure that all employees are aware of current security risks.
6. The effectiveness of training is evaluated and recorded by the organization. Training records are maintained to demonstrate competency and experience.
7. All staff are required to attend, at least annually, general security awareness and other such programs as deemed necessary by the organization.

Internal Reference Documents

Information Security Awareness Training Standards and Procedures

External References

NIST Special Publication 800-50, “Building an Information Technology Security Awareness and Training Program.” October, 2004.

ISO/IEC 27002:2013, 2nd Ed. Section 7 Human Resource Security: 7.2.2 Information security awareness, education and training

Access Control

Objective

To appropriately limit logical and physical access to information and information processing facilities. Access control policies help to ensure access to systems, services and physical facilities is approved and authorized, as well as helping to ensure that unauthorized access is prevented.

Policy

1. Access control policies are documented and reviewed based on business and information security requirements.
2. Asset owners are involved in determining appropriate access control rules, restrictions for specific user roles, and the appropriate level of detail and strictness based on the associated information security risks.
3. There is segregation of access control roles (i.e., access request, access authorization and access administration). No single individual or group may perform more than one role; for example, an access requestor may not also grant access or authorize it.
4. Access is granted based on the principle of least privilege / minimum necessary. All access is generally prohibited unless specifically granted. This access includes physical as well as logical access. Staff members are only granted the minimum access required for their job functions.
5. Staff access is role based, and access must be strictly tied to the specific job functions to be performed. Any additional access over and above role-based access must be formally requested and authorized.

6. All access must be formally approved and authorized by the business owner of the asset to which access is being requested. Such requests must be documented and evidence of request and approval maintained for evidentiary and auditing purposes.

7. All access to physical locations, particularly those housing systems that store or process data, provide application or administrative services, contain network infrastructure devices, etc.is considered privileged and as such must be authorized and approved by the business owner, staff member's manager, CTO or CFO and/or CISO as appropriate based on the information security risk.

8. All users are provided access to network and network services based on the principle of least privilege and will only be granted access to such networks and services based on specific authorization. This includes, but is not limited to:

    - Use of remote access technology
    - VPN or wireless network use
    - Monitoring or tracking use of network services
    - Specific application services used for administration or monitoring of systems and networks

8. Management of access rights will ensure that access remains consistent and appropriate in a distributed and networked environment, regardless of types of connections available.

9. Where network connections are not appropriately secured to the level of access required (i.e., access to sensitive data over an unsecured network connection), connections over this network are disallowed.

Automatic Logoff Policy

Automatic logoff is used to ensure that access to the organization's systems or data is not allowed through the use of unattended devices, or through display of such data in a public location.

1. All systems (including servers, network devices, workstations, laptops, etc.) are configured to enforce automatic logoff or password protection.

2. Devices, including workstations, laptops, tablets, etc.that process or display confidential, sensitive or regulated data, must be located in a physically secure location wherever possible.

3. Where such physical security is not possible, devices may be required to implement an automatic logoff or screen lock in less than ten minutes, as determined by risk assessment and sensitivity of data being accessed.

4. All applications that process, transmit or capture sensitive or regulated data must enforce a session or application timeout. Where this cannot be done due to technical considerations, compensating controls must be reviewed by the CISO or designee and implemented.

5. Remote access and administrative console activity are considered to be sensitive in nature and will implement an automatic logoff or session termination.

Internal Reference Documents

Access Control Standards and Procedures

External References

ISO/IEC 27002:2013, 2nd Ed. Section 9 Access Control: Section 9.1; Section 9.1.2

Access Management

Objective

To ensure that appropriate registration, deregistration and recertification processes are implemented. User access management will follow appropriate procedures for user identification, account use, etc. as appropriate, based on the sensitivity of information assets and/or information systems and facilities.

Policy

1. User registration and de-registration (creation and disabling/purging) must be documented, authorized and approved by business owners of information assets to enable assignment of access rights. (See also Workforce Security Policy.)

2. Access will not be activated either internally or by service providers prior to the completion of authorization and approval processes.

3. All user access is removed in a timely manner upon separation or termination from the organization. Privileged and/or administrative access is immediately removed or disabled and evidence of such removal is retained for auditing purposes.

4. Changes in user access must be formally requested and approved.

5. User access to any and all systems must satisfy, at a minimum, a user authentication mechanism such as a unique user identification and password.

6. Users with specific access to confidential, sensitive or regulated data or systems storing and/or processing this data must satisfy additional authentication mechanisms, such as biometric input, a user identification token, etc.to verify their authenticity.

7. A record of all access granted to information systems and services is retained centrally for regular review.

8. Users may not misrepresent themselves when accessing the organization's network or information assets by the use of another individual's unique identifier and password (User ID and password); nor may the user seek access to the organization's confidential, sensitive or regulated information assets or systems by the use of additional authentication mechanisms as noted above.

9. Users are responsible for the use made by others of their access and may not allow other individuals to access systems using their assigned unique identifier.

Account Management

1. Accounts will follow specific guidelines to ensure that appropriate security is maintained in their use.

2. All accounts are assigned to a specific individual. That information is maintained as part of the account and user registration record.

3. Generic accounts are specifically disallowed, except as required by technological restrictions or business use. Generic accounts must be reviewed and approved by the business owner, the CTO and CISO or designee as appropriate.

    a. Generic accounts used for client access is permitted as required by the business, but must be audited periodically or compensating controls such as monitoring and alerting on use of the generic accounts must be implemented and regularly audited for effectiveness.

4. Information security depends on personal accountability, therefore the requesting business owner remains personally accountable for the use of the generic account.

5. Generic accounts are restricted to the least privilege required for their intended function. The account will follow the password policy based on the level of access granted and must be changed timely in accordance with the password criteria.

6. IT Operation and administrative staff may be required to have knowledge of accounts used for sensitive automated processing or as application or system service accounts. These accounts must be appropriately secured and follow the organization's password criteria. These accounts' password must be changed whenever any staff member with knowledge of such account information is separated or changes job functions.

7. The generic login account password will follow the organization's password criteria and the password will also be changed whenever the business owner of this account changes, or staff members with knowledge of the account information are separated or change job functions.

Password Criteria

Passwords are a commonly used type of secret authentication and are a major means of user verification. As such, passwords must be appropriately secured based on the level of access being verified by the user login/password combination.

1. All user passwords will be reasonably complex to help ensure passwords are not easily guessed.

2. Passwords must be unique and not employ common phrases, words commonly found in any language dictionary, or commonly used names that could be associated with the employee, the organization's business or physical location (such as a sports team name, common business acronym, etc.).

3. Each user will be assigned a unique account and password that may not be shared with another individual.

4. All passwords must be stored in a secure manner by the underlying operating system, authentication method, such as a single sign on solution, or cloud-based services. Additionally, any password manager, such as DashLane, LastPass, etc., must employ secure encryption methods, as well as provide secure access, such as two factor authentication. Password managers must also provide secure user role management.

5. Employees must use discrete, unique passwords for all assigned accounts and may not use a password that is also used for a personal account.

6. Initial passwords or account provisioning links must be securely communicated to the workforce member and will be configured to expire within 24 hours.

7. Accounts with access to information processing systems and confidential, sensitive or regulated data will have additional password restrictions as deemed appropriate. This will include:
    a. Password length of ten (10) characters, and follow all other aforementioned rules.
    b. Must be changed every 90 days or the account must use multi-factor authentication (MFA). If multi-factor authentication is used, then passwords do not need to be changed unless they are known to be compromised.
8. When passwords cannot be changed on a regular basis due to technological considerations and MFA can not be used (service accounts, accounts used for

automated processing, etc.), password length and strength may be increased; this exception to the policy must be approved by the CTO or CFO and CISO.

9. User passwords that cannot be changed as per the password policy and do not employ MFA, must in no event, exceed a password age of 90 days.
10. Passwords for default accounts will be changed immediately and will always be configured to use the more secure settings of accounts with sensitive access.
11. Password settings and frequency of change will be enforced using access administration systems, (operating system password configuration, application user configuration settings, etc.).
12. Passwords must be changed whenever the security of the password is in doubt; for example, when it appears there has been unauthorized access using the associated account.

Access Review and Recertification

1. Access should be reviewed and recertified at regular intervals to ensure that access is appropriate, and that unauthorized access has not been obtained.

2. Asset owners and staff managers are responsible for access review upon changes, such as promotion, demotion or termination of employment. This includes access review for all applications, services, etc. HR may conduct authorization recertifications.

3. Business managers are responsible for the review of user access and for formally recertifying that such access is accurate. HR may conduct authorization recertifications.

4. Privileged access to confidential, sensitive or regulated data or administrative access to systems or applications is reviewed and recertified on a more frequent interval. Such access is reviewed and recertified by the business manager or VP of People as well as the CTO and CISO as appropriate.

5. Where access must be revoked, changed or otherwise re-allocated, the staff manager is responsible for identifying how the access is to be changed and for ensuring that such changes are made timely.

6. The business managers and owner responsible for generic accounts are responsible for the review and recertification of these accounts to ensure that access is appropriate and the account is still being used.

7. When generic accounts are no longer required or the access is changed or otherwise re-allocated, the business owner is responsible for identifying the changes and ensuring that these have been made timely.

8. Evidence of the review and recertification process is retained as deemed necessary to comply with industry standards, federal and/or state privacy regulations.

Internal Reference Documents

Access Management Standards and Procedures

External References

ISO/IEC 27002:2013, 2nd Ed. Section 9 User Access Management: Sections 9.2.1-9.2.6 inclusive.

ISO/IEC 27002:2013, 2nd Ed. Section 9 User Access Management: Sections 9.3 User Responsibilities.

Physical/Environmental Security

Objective

To prevent unauthorized physical access, damage or interference with the organization's information and information processing facilities.

Where information assets are stored, processed and transmitted by cloud service providers (Including but not limited to IaaS, SaaS, PaaS), the policy statements here are used to ensure that these vendors maintain a program that meets these security objectives.

Policy

1. The site location and strength of the perimeters is based on the security requirements of the assets within the perimeter. Where the risk to information assets is low, less stringent security is required.
2. Physical security perimeters are defined based on the risk associated to those areas containing sensitive or critical information and information processing systems.
    a. Physical access control systems such as badging systems, security access control, CCTV monitoring systems that enable access to physical areas are considered sensitive systems and protected as such. This includes separate security and authorization for access.
        i. Where manual keys are used to secure office space, cabinets and office rooms must be appropriately secured and access controlled.
3. All access to the organization's facilities is logged and monitored as appropriate based on the associated information security risk.

a. Monitoring of facilities is done in a manner consistent with the level of information security risk associated with the information stored or processed. This monitoring may include based on the risk associated with the facility, but is not limited to:

    i. Physical patrol by security professionals
    ii. Alarms at secured doors that are monitored and that generate a response by police or other security personnel
    iii. Monitoring by means of closed-circuit television (CCTV); such recording is retained based on the level of risk and as required by compliance to industry standards, federal and/or state regulations
    iv. All monitoring and logging of physical access systems and video recording will be retained for evidentiary purposes as deemed appropriate

4. For information assets classified as Confidential or higher, the following is enforced at a minimum:

    a. Access to general areas of the organization will be logged with the date and time of entry and departure.
    b. All visitors are supervised and escorted unless their access has been previously approved; such access should be granted for specific authorized purposes and may be monitored as deemed appropriate.
    c. Access to areas containing confidential, sensitive or regulated information is restricted to internal staff unless explicitly approved by the CISO or designee.
    d. Separate logging of visitors to areas containing information processing facilities, and confidential, sensitive or regulated data is done; this access is monitored and visitors are escorted at all times

5. Physical security for building or site containing information processing facilities that include but are not limited to data centers, offices and call centers should be physically sound, including but not limited to:

    a. No gaps in the perimeter or areas where a break-in could occur
    b. Exterior roof, walls and flooring should be of solid construction
    c. Information processing facilities should have walls that separate the site from other areas within the facility and that leave no gap between one floor and the next.
    d. Doors are appropriately secured with keys or other access mechanisms including card readers and pin entry devices
    e. Fire doors on a security perimeter should be alarmed, monitored and

tested to ensure the required level of resistance in accordance with suitable standards and should operate in accordance with local fire code in a failsafe manner.

f. Fire alarms and fire suppression in accordance with local fire code is required.
g. Physical protection from other environmental factors, such as natural disaster or malicious attack, is considered and applied based on the risk assessment.
h. Where appropriate as deemed by risk assessment, a manned reception area or equivalent is present to secure access to the organization's facilities.
i. Third-party, external support service personnel are granted restricted access only as required and such access is monitored and requires prior approval.

6. Physical security for building or site containing information processing facilities that include IT assets such as servers, major network infrastructure systems.

    a. Power conditioning and backup are in place for all critical systems to keep such systems online, and are considered and applied based on the risk assessment.
    b. Environmental controls such as HVAC to protect critical systems from environmental factors are implemented based on risk assessment.
    c. Access to delivery and mail facilities from outside the facility is restricted and separated from all areas containing systems processing, transmitting or storing sensitive information.

7. Where information processing facilities are managed by external parties (ie. landlords; facilities management companies, co-working spaces), the considerations for physical and environmental security must meet the requirements of the organization.

8. The organization retains responsibility for review, authorization and termination of access to information processing facilities. This stands even if the operations or technology is provided or maintained by a third party.

Internal Reference Documents

Physical/Environmental Security Standards and Procedures

External References

ISO/IEC 27002:2013, 2nd Ed. Section 11 Physical and Environment Security: Section 11.1 Secure Areas.

Change Management

Objective

To ensure that all changes are authorized, approved and reviewed to ensure that the risk of instability to the environment is considered. In addition, security concerns related to the confidentiality, integrity and availability of data are considered, and risks are mitigated to an acceptable level.

Policy

Changes to business critical systems and infrastructure that are not properly controlled and tested can cause instability or loss of information processing. This may result in data breaches, business reputation or revenue loss due to unavailability of applications or systems, loss of revenue due to fines, litigation, etc.

All changes to network infrastructure, either physical or virtual, significant updates to third-party systems, internally developed systems, particularly those that are business and mission critical must be controlled and tested depending on the level of risk to the organization. Therefore, it is important that all changes:

- ➢ are appropriately requested, documented and authorized by business management or designee(s) in writing as applicable for the level of effort and cost of the change.
- ➢ are categorized as “Minor”, “Major”, “Routine or Business-as-Usual (BAU)”, and “Emergency.”
- ➢ have security concerns and changes reviewed by the CISO or designee as appropriate and are approved or revised as needed.
- ➢ undergo planning and testing appropriate to the impact of the change.
- ➢ maintain project plans for significant changes as part of the change process where appropriate and defined timelines and objectives are met.
- ➢ undergo appropriate assessment of potential impacts.
- ➢ consider the availability of appropriate resources to implement and support changes being implemented.
- ➢ meet business expectations.
- ➢ include documentation for fall-back processes (where non-obvious), including procedures and responsibilities for aborting and recovering from unsuccessful changes and/or unforeseen events.
- ➢ have change details communicated to all relevant parties.

- ensure that there is appropriate notification to end users of system status due to changes being implemented.

1. Executive management authorizes and supports the implementation of a Steering Committee or equivalent procedure that represents all areas of business and has the technical expertise to make informed decisions.

2. All changes to systems, infrastructure, etc. are authorized and approved by business management before being submitted to the Change Management process.

3. All changes are submitted to the Change Management process and their details documented.

4. All changes are categorized appropriately to the level of effort required to ensure appropriate review, testing is done and resources are allocated.

5. Security requirements are considered and approved by the CISO or designee for all changes as appropriate, and are evaluated and approved again prior to implementation.

6. The impact of all changes is reviewed by appropriate staff members with consideration for the stability of systems, availability of systems for business processing, and resource allocation for implementation of the changes:

7. All significant impacts must be addressed through fall-back procedures or other mitigation, including additional testing, additional resources allocated for the change, etc.

8. Testing must be conducted according to the Testing Policy, standards and procedures and may not include the use of any sensitive, regulated data. If use of such data is required, the data must be masked, obfuscated, tokenized or encrypted according to Data Classification Policy and/or using the highest level of protection for the sensitivity of the data in use. (See Testing Policy, Standards and Procedures)

9. All testing must be performed in segregated environments as per the Testing Policy and as applicable to the impact of the change (see Testing Policy, Standards and Procedures.) Testing may be completed directly on office production environments, but should be minimised.

10. If testing of infrastructure or system changes cannot be performed in separate, segregated environments, alternate testing plans must be developed and reviewed. These may include but are not limited to:
    a. restricted testing in a specific subset of the production environment
    b. research into potential effects of changes in environments similar to the organization's, such as the effect of vendor issued updates, security patches etc., as documented on well-known industry websites.

1. All issues found during testing must be addressed prior to final approval for implementation.
2. Changes are reviewed and approved by the Steering Committee or individual designees as appropriate. All such approvals must be documented.
3. No approvals may be done by the requester of the change in order to ensure the principle of segregation of duties is maintained.
4. Separate approval by the CISO or designee must be obtained for major changes affecting information systems that process sensitive, regulated data.
5. There must be communication to all stakeholders, information systems prior to implementation into the production environment. End users will be notified if changes have an impact on them.

Internal Reference Documents

Change Management Standards and Procedures

External References

ISO/IEC 27002:2013, 2nd Ed. Section 12.1.2 Change management.

Testing

Objective

To ensure that testing of all development or other changes to systems, infrastructure, etc. is complete, that all testing is reviewed and approved, and that appropriate security is applied. Such security includes, but is not limited to, segregation of duties and environments, security of test data being used, and appropriate monitoring of test accounts and accounts used to implement changes.

Policy

1. Testing is performed by staff with appropriate training and knowledge of systems.
2. Test environments are segregated from the production environment. Test environments are also segregated from other test environments, ensuring that each environment contains a discrete authorized version of software, security or system updates, and infrastructure being tested.
3. Test scripts are created as needed and appropriate to requirements. This may include regression testing, load testing, security testing of configuration, administration, etc.

4. Testing is reviewed by authorized individuals for completeness and accuracy. All testing is documented and such documentation is retained until changes have been implemented in the production environment and normalized.
5. All versions of testing, including development changes, configuration of systems, software and/or OS updates, etc. are finalized and may not be changed after final review.
6. Version control is maintained between test environments and between the final test environment and production.
7. Data used for testing will not include any sensitive, confidential or regulated data. All data is completely deleted and scrubbed prior to migration between test environments, and prior to implementation in the production environment.
8. In the event that test data must contain sensitive, confidential or regulated data for appropriate testing, the CISO or designee will authorize this use.
9. Such data is protected based on the data classification level. This includes tokenization, encryption, additional access controls, etc. Separate tokenization systems, encryption keys, etc. from those used in other test environments or in the production environment are used. Access to such data is approved by the business manager and reviewed in the same manner as access to production data.
10. All references to test accounts in scripts, application code, etc. are deleted, or code is maintained in a way that this information does not enter production code (e.g. through the use of environment variables or configuration management systems).
11. Test accounts and those accounts used to migrate changes between test environments and into the production environment are appropriately monitored.
12. Post implementation testing is performed as needed and results documented. Such documentation is maintained until all changes have been normalized.

External Reference

ISO/IEC 27002:2013, 2nd Ed. Section 12.1.4 Separation of development, testing and operational environments.

Software Development Life Cycle

Objective

Software and information systems are used to process, store and transmit sensitive data and act as systems of record for a variety of business critical functions. These systems are critical to business objectives and therefore their development must ensure that they meet business criteria, all objectives are met and security is appropriately considered at all phases of development, enhancement and replacement. To ensure that information systems are appropriately considered and secured, the following key points are identified:

- ➢ All organization software and web application or upgrades involving the handling and/or access of sensitive information must be reviewed and approved by the CISO or designee(s) via Steering Committee or Vendor Process in writing at the requirements phase of implementation.
- ➢ Security is considered and becomes an integral part of information systems
- ➢ Software meets business purposes
- ➢ Development project timelines and objectives are met
- ➢ Errors and defects in development are kept to a minimum
- ➢ Resources are appropriately assigned
- ➢ Business expectations are met
- ➢ End user expectations and satisfaction with goals of software are met

Policy

1. All development initiatives are requested by the business owner and such requests are documented.

2. Business requirements and technical specifications required for development are documented and retained as part of the SDLC artifacts. Technical specifications must also include finalized security requirements as designated by CISO or designee.

3. [7]Security requirements are considered and approved by the CISO or designee at initiation and evaluated and approved again at all major project milestones.

4. Secure application coding processes are used, including:

    a. Processing controls must be designed into applications that process sensitive data to ensure correct processing. These include validation of input data, such as missing data, incomplete data, out of range values, etc.

[7] "ISO_IEC_27002_2013(En).PDF," n.d., secs. 14.1.1-14.1.3.

b. Secure coding guidelines must be developed and maintained for all programming languages in use.
c. Code repositories must be secured appropriately against unauthorized access and disallow unauthorized compilation, approval or migration of code into production or other environments.
d. All web applications that process, store or transmit sensitive data, the systems and networks supporting the applications must be scanned for technical vulnerabilities at a minimum. All vulnerabilities exceeding CVSS score of 4.0 or above must be remediated prior to implementation into the production environment.
e. Developers must be provided sufficient training in secure coding techniques (See Training Policy) and be familiar with countermeasures for web application vulnerabilities such as those documented in the OWASP (Open Web Application Security Project) and other industry bodies.[8]
f. System security plans and documentation must be prepared for all company information systems or other systems under development that require special attention to security due to the risk of harm resulting from loss, misuse, or unauthorized access to or modification of the information being processed by the system(s). Such plans should provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements through all stages of the system's life cycle. When the system is modified in a manner that affects security, system documentation must be updated accordingly.

5. All testing performed must be performed in segregated environments and according to the Testing Policy, Standards and Procedures. (See Testing Policy.)

6. All defects found during QA and UAT testing are evaluated as to impact and prioritized for remediation. They are all tracked using the QA application of record through to closure.

7. The implementation of all changes to environments, including Development, Test, QA, UAT, and any other applicable environment is performed by authorized personnel with appropriate access privileges.

8. No live or unmasked data should be used for testing. If testing cannot be completed without live data, this data must be handled in accordance with the highest applicable level of classification. This may include masking, obfuscation, encryption, tokenization, etc. (See Data Classification Policy and Data Management Policy.)

9. There must be formal approval by CISO or designee in addition to Business Owner prior to implementation into the production environment.

[8] "ISO_IEC_27002_2013(En).PDF," secs. 14.2.1-14.2.4.

Internal Reference Documents

SDLC Standards and Procedures

External References

ISO/IEC 27002:2013, 2nd Ed. Section 14.1 Security requirements of information systems, 14.2 Security in development and support processes

IT Operations

Objective

To ensure the correct and secure operations of processing facilities.

Policy

1. All operational procedures are documented and made available to those staff members.
2. Documented procedures are prepared for operational activities associated with information processing and communication facilities, including but not limited to: computer start-up and close-down procedures; backup; equipment maintenance; media handling; computer room and mail handling management; and safety.
3. The operating procedures should specify the operational instructions including, but not limited to:
    - ➢ The installation and configuration of systems
    - ➢ Processing and handling of information both automated and manual
    - ➢ Backup and restoration (See Data Backup and Restore)
    - ➢ Scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times
    - ➢ Instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities
    - ➢ Support and escalation contacts including external support contacts in the event of unexpected operational or technical difficulties
    - ➢ Special output and media handling instructions, and the management of confidential output including procedures for secure disposal of output from failed jobs (see Document Management and Data Management Policies)
    - ➢ System restart and recovery procedures for use in the event of system failure
    - ➢ The management of audit-trail and system log information as well as monitoring processes (see Logging and Monitoring)

4. Operating procedures and the documented procedures for system activities should be treated as formal documents and changes authorized by appropriate team member.. Where technically feasible, information systems should be managed consistently, using the same procedures, tools and utilities.

Capacity Planning

1. Capacity requirements are identified and documented.
2. Capacity for key information systems is documented and a capacity management plan is created and updated.
3. Utilization of key resources is monitored and reviewed on a regular basis.
4. Dependencies on key personnel resources are considered and planned.
5. Management of capacity planning is documented and includes, but is not limited to:
    - ➢ Deletion of obsolete data
    - ➢ Decommissioning of obsolete systems, applications and environments
    - ➢ Optimizing scheduled processes and batch processes
    - ➢ Optimizing application or database logic or queries
    - ➢ Denying or restricting bandwidth to non-essential applications

Infrastructure Security

Network

1. Network security is implemented to ensure the security of confidential, sensitive or regulated data being transmitted on networks, and stored and/or processed on systems residing on networks.
2. Operational responsibilities and procedures for networking infrastructure are established to ensure secure operations.
3. Responsibilities for computer operations and networking operations are segregated.
4. Network access control lists or their equivalent (ex: AWS Security Groups) that transmit from less secure to secure (inbound), default to “deny all” except for those networks that are specifically allowed access.
5. Networks and systems containing or transmitting confidential, sensitive or regulated data are segregated from other networks through the use of firewalls, secure VPNs, etc.

The access control lists for these devices contain only approved inbound and outbound addresses and are configured to otherwise "deny all."

6. If SNMP is implemented, the default communities and passwords must be changed and these passwords must follow the organization's password criteria as well as maximum password age.

7. Logging and monitoring is implemented to detect malicious activities.

8. Network management activities are handled to minimize the interruption of service and are approved and authorized through the Change Management process. (See Change Management Policy and Change Management Standards and Procedures.)

9. Wireless networks are secured with strong encryption when transmitting confidential, sensitive or regulated data.

10. Only authorized and approved wireless networks are allowed to connect to the organization's network

11. A guest network for general use will have no connection to the organization's internal network and is segregated through the use of firewalls.

12. All network services are kept to the minimum possible and are documented as to the reason for the service.

13. Systems and wireless network devices are restricted from connection to the organization's network without appropriate authorization and approval.

Server

1. All server hardware and software is reviewed at a period determined by executive management based on risk assessment so that no out-of-date software or hardware remains in service.

2. Virtualized servers are implemented from a fully reviewed and secured image. Images from which servers are implemented are reviewed periodically based on security and compliance requirements and updated with current security updates.

3. Servers are configured with the minimum number of services as required by their business function.

4. Servers are configured for one function only (i.e., administration, email, web server, database, etc.).

5. Servers are restricted from connection to the organization's network without appropriate authorization and approval. All servers must be approved through the Change Management process.

Workstation

1. For purposes of this policy, the term workstation refers to desktop computers, laptops, tablets and other devices (excluding SmartPhones) which are used to transmit, process or access data for business purposes. This policy applies to devices owned by the organization, as well as those owned by workforce members.
2. Workstations must have licensed and approved software installed.
3. Workstations are configured to provide only those applications required by staff members using the device.
4. Workstations that are used to administer computer devices must be on a secured VPN that is protected by appropriate segmentation and/or firewalls.
5. Images used for implementation of workstations must be reviewed on a quarterly basis and updated as needed.
6. All workstation hardware and software is reviewed to ensure that it is current and no out of date software or hardware is in use.
7. All workstations must be hardened, including but not limited to full disk encryption and antivirus.

Mobile Devices

For the purposes of this policy mobile devices refers to SmartPhones, such as Android, iPhone and Windows Phones. All other devices such as laptops and tablets are considered to be workstations.

1. Mobile devices cannot be "rooted.[9]"
2. The device must be configured to be managed centrally.
3. The device must be configured to lock itself after a predetermined period of time.
4. The mobile device must be configured with a pin or passphrase.

[9] "Rooting (Android) - Wikipedia." https://en.wikipedia.org/wiki/Rooting_(Android). January 22, 2018.

5. Applications that are installed must be from an approved list of applications. The organization's internal applications developed for mobile devices must be installed from the internal network or dedicated mobile application store.

6. When the mobile device is used to access applications processing or transmitting confidential, sensitive or regulated data, use of the camera or location finding applications must be appropriately restricted.

7. Mobile devices must be configured for strong encryption and all applications accessing the organization's network, information assets, etc.must utilize digital certificates.

8. All mobile devices must be securely wiped of data when being disposed or reassigned.[10]

9. All mobile devices must be remotely wiped in the event that the device is lost.[11]

Configuration and Hardening

For purposes of this policy, all infrastructure systems, including network devices (such as routers, firewalls, etc.), servers, virtualized servers, workstations, and mobile devices are considered to be a device.

1. All devices are configured with only the services specific to the function of the device.

2. Insecure services or applications will not be installed.

3. Initial configuration of the device will include all security updates, including those for applications, services, etc.

4. Default user accounts and passwords are disabled and/or reset from the default.

5. All devices are configured in accordance with industry standard secure configuration standards such as CIS (Center for Internet Security), SANS (SysAdmin Audit Network Security) or NIST.

Patch Management

1. The CTO/CFO or designee is responsible for implementation of a security and system update process.

2. Reliable external sources are used as reference for security vulnerability information.

3. The CTO and staff review updates as required and plan regular implementation.

---

[10] "Guidelines for Media Sanitization - Nvlpubs.nist.gov…." 1 Dec. 2014, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf. December, 2014

[11] Although remote wiping of a device is not the most secure method, this does reduce the risk that data will be accessed.

4. All security updates that are considered as critical, high or medium risk ranking for operating systems, applications, infrastructure devices, etc. are applied timely.

5. Processes are in place to ensure that system stability and availability are not affected by updates.

Malware and Antivirus

1. Antivirus and malware software are installed on all servers, workstations and mobile devices and are centrally managed by the organization.

2. Software is kept current with updated signatures and new versions as needed.

3. Antivirus software is configured to scan continuously if possible. Where not technically possible, scans are executed periodically at a frequency designed to minimize risk to information systems.

4. Antivirus/malware software is configured so that end users cannot disable software or alter configurations.

5. Software is configured to maintain logs centrally of updates, viruses discovered, cleaned or quarantined, etc. The logs are retained for a period as required by compliance and security best practices..

Vulnerability Management

The development, implementation and execution of the vulnerability assessment process is the responsibility of the Chief Information Security Officer (CISO).

1. Vulnerability scans are performed periodically on all network assets deployed within the organization’s environment.

2. The organization must conduct vulnerability testing on all systems on a regularly scheduled basis. Upon any configuration change to the system, an internal scan must be performed. Failed vulnerability scans must be addressed and followed by a retest.

3. All issues found during the performance of a vulnerability assessment are documented on the organization's risk register and are managed in accordance with the Risk Management Policy.

4. Metrics are reported to management as part of the ongoing Security Risk Management Program.

Penetration Testing

1. External and internal penetration testing shall be performed at least once a year.

2. External and internal penetration testing shall be performed after any significant infrastructure or application changes.
3. Penetration testing shall minimally consist of network-layer and application-layer penetration tests.
4. All issues from penetration testing will be documented on the organization's risk register and will be managed in accordance with the Risk Management Policy.
5. Metrics will be reported to management as part of the ongoing Security Risk Management Program.

Internal Reference Documents

IT Operations Standards and Procedures

External References

ISO/IEC 27002:2013, 2nd Ed. Section 12 Operations Security: 12.1 Operational procedures and responsibilities; 12.1.3 Capacity management; 12.2 Protection from malware; 12.5.1 Installation of software on operational systems; 12.6.1 Management of technical vulnerabilities; 12.6.2 Restrictions on software installation.

ISO/IEC 27002:2013, 2nd Ed. Section 13 Communications security: 13.1.1 Network controls; 13.1.2 Security of network services; 13.1.3 Segregation in networks.

Encryption

Objective

To ensure that sensitive, confidential or regulated data is secured from unauthorized access and to affect the confidentiality, integrity and non-repudiation of sensitive data and transactions.

Policy

1. The use of encryption to control access to data is determined by the data classification level and the potential risk to the organization based on data exposure.
2. The use and level of encryption is based on a risk assessment; the required level of protection is identified taking into account the type, strength and quality of the encryption algorithm required.
3. The same key cannot be used both for encryption of data (confidentiality) purposes and also for digital signatures of transactions (non-repudiation or authentication.)

4. Encryption is used for the protection of information transported by mobile or removable media devices or across communication lines. The level of encryption is based on the level of protection required by the information asset as designated by the data classification level.

5. The distribution of keys and overall key management is handled in a secure manner as described in the Key Management Policy.

6. Encryption and the algorithms in use is subject to all national and international regulations that apply, and all considerations relevant to the transmission across borders of encrypted data.

Internal Reference Documents

Encryption Standards and Procedures

External References

ISO/IEC 27002:2013, 2nd Ed. Section 10 Cryptography: 10.1 Cryptographic controls; 10.1.1 Policy on the use of cryptographic controls.

NIST Special Publication 800-57 Part 1 Revision 4, “Recommendation for Key Management Part 1: General”, January 2016.

Key Management

Objective

To ensure that the keys used to encrypt confidential, sensitive or regulated data are adequately protected and that all data requiring encryption is encrypted using controls that meet operational needs and comply with data recovery requirements. This policy includes keys that are used to encrypt data (data encryption keys) as well as those being used to encrypt keys while in transit or when stored (key encryption keys). This policy and related standards and procedures help to ensure that keys are created, managed and accessed in a secure manner and consider the requirements of data recovery, data retention, and key requirements for confidentiality and non-repudiation.

Policy

1. Key management is fully automated wherever possible to ensure that unauthorized staff do not have the opportunity to expose a key or influence the key creation.
2. Exceptions to full automation must be approved by the CISO and must be strictly managed and audited.
3. The concept of least privilege is used for personnel managing, distributing and creating, either data encryption keys (DEK) or key encryption keys (KEK).
4. Segregation of duties are enforced in key management processes; separate roles are created and used for the creation of keys, management of profiles, and use of keys.
5. The CISO verifies backup storage for key passwords, files, and related backup configuration data to avoid single point of failure and ensure access to encrypted data. This includes all key data required for data retained archivally for business purposes.
6. No single individual or role is responsible for any process or knowledge of an encryption key. Dual control or split knowledge must be implemented. Dual control requires that at least two people control a single process, such as enabling access to master encryption keys. Split knowledge provides only partial knowledge of an encryption key or passcode to any one person, requiring action from multiple parties to access critical data.
7. No single individual is authorized to generate a new certification authority (CA) key pair.
8. Certificates must be issued by commercial and governmentally-approved authorities.
9. Private keys must be kept confidential; when using asymmetric keys, private keys are secured with strong access controls and held securely.
10. All users holding either the private key of an asymmetric key pair, or those with knowledge of symmetric key, will sign a formal acknowledgement of their responsibilities and this documentation will be retained as part of key management documentation.
11. Regular audit trail reviews of key management processes are conducted.
12. Complete, regular training on key management requirements and procedures will be provided as appropriate.
13. Keys in storage and transit must be encrypted.
14. Key encryption keys must be separate from data keys and not use the same passphrase.
15. Key encryption keys, if used, must be at least as strong as the data encryption key in order to ensure proper protection of the key that encrypts the data, as well as the data encrypted with that key.

16. If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not use the same user account authenticator as the operating system, or use a decryption key that is associated with or derived from the system's local user account database or general network login credentials.

Key Rotation

1. The cryptoperiod or the duration of the key validity is determined by the data classification of the information systems, transmission methods and data being encrypted. This may also be determined by various industry standards and state and/or federal regulations.

2. In order to provide a high level of security, keys must be rotated and changed regularly. Expired keys must be retained throughout the lifecycle of the sensitive data they are used to encrypt.

Internal Reference Documents

Key Management Standards and Procedures

External References

ISO/IEC 27002:2013, 2nd Ed. Section 10 Cryptography: 10.1 Cryptographic controls; 10.1.2 Key management

NIST Special Publication 800-57 Part 2 Revision 4, "Recommendation for Key Management – Part 2: Best Practices for Key Management Organization."

Acceptable Use

Please refer to the Information Security and Acceptable Use Policy for details.

Logging and Monitoring

Objective

To ensure that significant events are recorded sufficiently to monitor activity and generate evidence.

Policy

Logging

1. All systems within the organization or security domain are synchronized to a single reference time source to ensure the accuracy of time representation, i.e., NTP; time.nist.gov.

2. All information systems containing sensitive, confidential or regulated data, as well as network infrastructure involved in the transmission of such data, are configured to log sufficient information to validate activity.

3. General use systems, such as email, file storage systems, application development systems, etc. also have logging enabled.

4. Based on the criticality of the systems or data, exceptions to normal activity are defined and specifically monitored.

5. All information systems and network infrastructure devices containing sensitive, confidential or regulated data are configured to log all activity. Systems performing security and administrative functions are also included in this logging. The information captured must be sufficient for analysis and determining the initiator of the activity, type of activity, system exceptions, etc. This includes but is not limited to:
    a. User IDs
    b. System activity
    c. Dates, times and details of key events
    d. Device identity or location
    e. Record of successful and unsuccessful system access or data modification/access attempts
    f. Changes to system configurations

6. All systems that generate logs are documented and the characteristics of the logs (i.e., generation format, application used to generate logs, relevant data points, etc.) are identified. Such documentation shall be maintained and kept current.

7. All logging information shall be consolidated to a centralized location. This may be a physical appliance or server or a cloud based solution. There is sufficient capacity to ensure a minimum of 90 days (three months) of information is available online. Up to one year of data are kept in an archived format, accessible as needed.

8. Transfer of logs to the centralized location is protected such that logs cannot be modified in transit.

9. Administrative access to modify the content of the the centralized logging server shall be restricted; IT operational staff do not have access to ensure segregation of duties.

10. Logged data are encrypted and access limited monitored appropriately to ensure file and record integrity.

11. Logs are not configured to capture sensitive data; for example, application logging should prevent the capture of information such as PHI, PII, etc.

12. Appropriate measures are taken to protect logs containing sensitive, confidential or regulated data when this must be captured as part of the log record. These measures are consistent with the data classification of the information being captured and may include tokenization, obfuscation, encryption, etc.

External References

ISO/IEC 27002:2013, 2nd Ed. Section 12 Operational Controls: 12.4.1 Event logging; 12.4.2 Protection of log information; 12.4.3 Administrator and operator logs; 12.4.4 Clock synchronisation

Monitoring

Monitoring is an integral part of ensuring unauthorized and potentially malicious activity. The organization, at a minimum, implements monitoring on all systems that process sensitive, confidential or regulated data, as well as the networks that provide access to these systems and transmit this data.

1. Monitoring of all systems that process confidential, sensitive or regulated data and the networks that provide access or transmit this data is real-time or as real-time as technologically possible.

2. The time-sensitivity of monitoring of general systems is identified and documented and performed as appropriate.

3. The CTO, CISO and other identified subject matter experts identify and determine security events of interest for inclusion in monitoring of sensitive systems, including:
   - ➢ Individual user accesses to confidential sensitive or regulated data
   - ➢ Actions taken by any individual with root, administrative, or other privileged access to sensitive data
   - ➢ Access to all audit trails and event logs
   - ➢ Invalid logical access attempts
   - ➢ Use of and changes to identification and authentication mechanisms, including but not limited to the creation of new accounts, elevation of privileges, and additions or deletions to accounts with root, administrative or other privileged access to sensitive data

- ➢ Initialization, stopping or pausing of audit logs
- ➢ Creation or deletion of system-level objects
- ➢ Pausing, changing or stopping intrusion detection/prevention systems, firewalls both network and personal, antivirus/malware software, etc.
- ➢ Failed system processes, such as backups, scheduled processing of sensitive data, etc.

4. Security systems, including but not limited to, intrusion detection/prevention, file integrity monitoring, access administration and authentication are monitored as critical systems.

5. The CTO or CFO , CISO and other identified subject matter experts also identify security events and the time requirements for general use systems, such as file systems, email, etc.

6. Monitoring requirements are reviewed at least annually and is based on risk management analysis, compliance to industry standards and federal and state regulatory mandates.

Internal References

Logging and Monitoring Standards and Procedures

External References

ISO/IEC 27002:2013, 2nd Ed. Section 12 Operational Controls: 12.4.2 Protection of log information

Incident Management

Objective

To establish an incident response capability that allows incident response to be correctly defined, and performed effectively, efficiently and consistently. This enables the organization to prevent adverse incidents through lessons learned and improve incident response capabilities over time.

Policy

The following definitions are commonly used when discussing incident management or incident response:

- **Event** - is an observable occurrence in a system, or network,[12] such as those identified in the Logging and Monitoring Policy.
- **Adverse Events** - are events with negative consequences, that may or may not be security related[13]. For example, system crashes or unauthorized use of system privileges may be caused by instability, or negligence and not necessarily through malicious activity.
- **Computer Security Incident** - is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.[14] These include: Distributed Denial of Service (DDoS) to crash a web server; spam encouraging opening of executables or reports that contain malware; unauthorized distribution or sale of sensitive data; and ransomware.

Only computer security incidents are considered for the purposes of this policy. Imminent threats to security are issues that are identified by reliable sources, such as well-known security sources, including NIST, anti-malware/anti-virus manufacturers, etc. that a specific incident is about to occur. For example, a zero-day malware attack or an increasing spread of an attack using a specific vulnerability, would be considered imminent threats and are to be handled as part of the Incident Management Policy.

1. The organization identifies incidents based on the results of log monitoring, vulnerability assessments, and risk assessment results.

2. The policy applies to all information assets and systems of the organization.

3. Incidents are categorized and prioritized. Executive management, in conjunction with business management as appropriate, reviews and approves incident categorization.

4. The CISO and Compliance/Privacy Officer are responsible for the development of an Incident Response Plan and for its continuing review and revision.

5. The plan includes the following:

    - Initiation of incident
    - Authority for incident response team:
        - confiscation or disconnection of equipment
        - additional monitoring of activity pursuant to incident
        - working with external resources such as forensic analysis specialists
    - Strategy for execution on plan
    - Identification of legal and forensic requirements

[12] "SP 800-61 Rev. 2, Computer Security Incident Handling Guide | CSRC." https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final. pg. 15.
[13] op.cit; https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final. pg. 15.

[14] op.cit; https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final. pg. 15.

- ➢ Evidence retention
- ➢ Communications both internally and externally
- ➢ Legal requirements for communication
- ➢ Reporting guidelines and requirements
- ➢ Metrics for measuring incident response and effectiveness
- ➢ Performance improvement measures measures
- ➢ Development of general procedures as well as standard operating procedures (technically-detailed procedures and checklists)

6. Executive management establishes an incident response team to execute on the Incident Response Plan.
7. The organization develops a communication method to communicate internally regarding incidents, expected activity of staff, etc.
8. Training in expected responses to incidents, reporting of incidents, etc. is provided to all staff as part of general security awareness training.
9. The organization develops a plan to communicate with clients as required contractually upon execution of the incident response plan and determination of potential breach of security to sensitive or regulated data.
10. Formal breach notification is the responsibility of the CISO and other designees of the organization.
11. The organization develops a plan to communicate with law enforcement and make other required notifications as mandated by industry standards, federal and state regulations.

External References

ISO/IEC 27002:2013, 2nd Ed. Section 16 Information security incident management: 16.1.1 Responsibilities and procedures.

NIST Special Publication 800-61 Revision 2, "Computer Security Incident Handling Guide", August, 2012: Chapter 2.

Business Continuity Management

Objective

To plan for interruptions in business operations that are of short duration, and to plan for longer interruptions as defined by the organization's Maximum Tolerable Outage (MTO); and to ensure that the organization business is operated in contingency mode with expected levels of information security and operations, based on criticality and sensitivity of information assets and systems.

Policy

Information security requirements are an essential part of all business continuity management. Access controls and protection of information assets must be considered as part of the overall contingency planning process, whether the organization maintains responsibility for information systems and contingency planning or whether a third party organization such as an IaaS, PaaS is being used to provide infrastructure and system services.

1. The organization identifies the business impact of an interruption of service and determines what services are critical to ensure the continued achievement of the business objectives.

2. The organization develops a Disaster Recovery/Business Continuity Plan (DR/BCP) that identifies the processes that are required to address the interruption of services. This plan includes:

    a. Identification of key processes and supporting systems
    b. Information assets and systems with their defined data classification level
    c. Defined Maximum Tolerable Outage (MTO), Recovery Time Objectives (RTO), Recovery Point Objectives (RPO) for each of the key processes and information systems identified as part of the business continuity process
    d. Roles or personnel responsible for performing the tasks of authorizing implementation of the plan, along with roles or personnel responsible for ensuring appropriate security of assets
    e. Roles or personnel that are responsible for communication with clients, vendors and regulatory bodies as required by federal and state regulations or contractual agreements
    f. Organization of Crisis Management Team, and roles and responsibilities of team for overall planning and implementation
    g. Detailed procedures for team members once DR/BCP plan is executed
    h. Detailed procedures for normalization and return to regular operations

3. The organization tests the Disaster Recovery/Business Continuity Plan at a minimum annually and reviews results to improve the overall effectiveness of the plan.

4. If the organization outsources infrastructure or services, the organization is responsible for ensuring that the service provider successfully tests all their internal and external applicable systems, applications and processes at least annually.

Internal Reference Documents

Disaster Recovery/Business Continuity Plan

External References

Draft NIST Special Publication 800-53 Revision 5,"Security and Privacy Controls for Information Systems and Organizations", 3.6 Contingency Planning.

ISO/IEC 27002:2013, 2nd Ed. Section 17 Information security aspects of business continuity management.

End