Securing Information Systems Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

Information and physical security help protect ABC Company's Information Resources and ensure system confidentiality, availability, and integrity.

# II. Purpose

This policy helps protect ABC Company’s assets and ensures our ability to continue business operations.

# III. Scope

This policy applies to all Staff that use ABC Company’s Information Resources.

# IV. Policy

Security rules and procedures protect important assets and support the overall ABC Company (Company) mission. Through selecting and applying appropriate safeguards, security helps the Company's mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets.

Company Staff must understand both their organizational mission and how each information system supports that mission. After a system's role is defined, the security requirements implicit in that role can be defined. Security can then be explicitly stated in terms of the Company's mission.

The following security mechanisms shall be implemented to ensure information security and protect against data leakage through e-mail, social networks, and instant messaging applications.

Technologies such as fingerprinting shall be employed to ensure sensitive information can’t be copied, printed, or e-mailed. Sensitive information shall not be copied, moved, or stored onto local hard drives or removable electronic media unless explicitly authorized for a defined business need. Products shall be used to protect against data leakage:

* Data loss prevention (DLP) identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage) through deep content inspection and with a centralized management framework.
* Network based DLP solutions shall scan network traffic such as e-mail and instant messages for sensitive data.
* Endpoint DLP products shall tag and monitor sensitive data on servers, desktops, mobile devices, and other technologies that store data.
* Discovery DLP solutions shall locate and identify sensitive data.

Access to systems with shared network infrastructure shall be restricted to authorized personnel in accordance with security policies, procedures and standards. Networks shared with external entities shall have a documented plan detailing the compensating controls used to separate network traffic between the organizations.

A. Information Systems Risk Management

Information systems control virtually all of Company’s major record-keeping functions. Risks are created by the unique nature of computers themselves. By concentrating information in one location, Company increases its risk of loss or damage. Another risk is access to information from remote locations. Company’s information systems must be able to positively identify the user, as well as ensure that the user is only able to access information and functions that have been authorized.

Security personnel must evaluate the costs and benefits of security in both monetary and non-monetary terms to ensure that the cost of controls does not exceed expected benefits. Security must be appropriate and proportionate to the value of and degree of reliance on the information systems and to the severity, probability, and extent of potential harm. Requirements for security vary, depending upon the particular information system. Security benefits do have both direct and indirect costs. Direct costs include purchasing, installing, and administering security measures, such as access control software.

Staff shall refer to the Risk Management Policy to ensure proper steps are taken to identify and reduce risks to acceptable levels.

B. Information System Life Cycle

ABC Company’s IT Department is responsible for developing, maintaining, and managing a Software Development Life Cycle (SDLC). Please refer to the Secure Software Development Lifecycle Policy for more information.

The disposal of hardware, software, and information requires special consideration. Refer to the Disposal Policy, Encryption Policy, Data Retention Policy, and Removable Media Policy for more information.

C. Audit and Monitoring Techniques

Where possible, the CSO shall use Certified Information Systems Auditors to audit the security controls of ABC Company’s Information Systems. Security audits shall be performed on an annual basis or more frequently if major changes occur to Information Resources. Refer to ABC Company’s Audit Policy for more information.

Monitoring systems and audit trails shall be used to prevent unauthorized personnel from accessing ABC Company’s Information Resources. Audit trails can also be used as an incident detection and response mechanism. Refer to the Audit Trails Policy for more information.

D. General Information Systems Security Procedures

ABC Company recommends common-sense protective measures to reduce the risk of loss, damage, or disclosure of information. The following guidelines identify Information Systems controls that assure that the system is properly used, resistant to disruptions, and reliable.

Access to information

* Use – users are a first line of defense and shall follow safe computing practices as outlined in the Acceptable Use Policy.
* Passwords – passwords are a key component to system security. Refer to the Password Policy for more information.
* Logon attempts – users shall be locked out after five consecutive invalid logon attempts within a 24-hour period. The lockout duration shall be at least 30 minutes or until a system administrator enables the user ID.
* Inactivity – users shall be automatically logged off after 15 minutes of inactivity.
* Screen savers - protected screen savers are required and shall be activated after 15 minutes of inactivity.
* Inactive IDs. User IDs that are inactive on the system for a period of three months must be disabled.
* Clear desk – Staff shall ensure sensitive information remains secure by clearing their desks when they will be away from their office, positioning monitors to prohibit unauthorized viewing, etc. See the Clear Desk Policy for more information.
* Media – media must be handled according to Removable Media Policy requirements.
* Data storage – computers and handheld devices contain hard drives and non-destructive memory that may contain sensitive information. Refer to the Encryption Policy, Mobile Device Policy, Smartphone Policy, and Wearable Computing Policy for requirements to keep unauthorized individuals from accessing such data.
* Third party access – prior to granting individuals physical or logical access to information resources, agreements with staff, third party users, and customers shall be in place and include responsibility for information security. Refer to the Third Party Service Providers Policy for more information.

Communications and operations

* Diagnostic ports – physical and logical access to diagnostic and configuration ports shall be controlled. Refer to the Network Configuration Policy and Physical Access Policy.
* Border routers – border routers may be used to filter traffic and protect against spoofed IP addresses.
* Firewalls – firewalls shall protect the network and limit traffic to only approved activities. For more information see the Firewall Policy.
* Location – access to Information Resources may be based upon physical or logical location. Similarly, users can be restricted based upon network addresses (e.g., internal users may be permitted greater access than those from outside the organization).
* Time – time and day restrictions may be used to limit access to data (e.g. access to personnel files may only be allowed during normal working hours).
* Transaction - transaction based access criteria can be used. For example, access to a particular account could be granted only for the duration of a transaction. When completed, the access authorization is terminated.
* Management – networks shall be managed and controlled to protect information in systems and applications.
* Services - only network ports, protocols, and services listening on a system with validated business needs, shall be running on each system. Host-based firewalls or port-filtering tools on end systems shall apply a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.
* Service levels – security mechanisms, service levels, and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.
* Segments – groups of information services, users, and information systems shall be segregated on networks.

Information security protection

* Access – access controls enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. IT security Staff shall protect information stored on systems with file system, network share, claims, application, or database specific Access Control Lists (ACL). ACLs are a register of users (e.g. groups, machines, processes) permitted to use a particular system resource and the types of access they have been permitted.
* Account management – policies and procedures shall manage the process of creating, monitoring, controlling, and removal of accounts. Refer to the Account Management Policy for more information.
* Acquisitions – only hardware or software acquired through ABC Company’s approved policies and procedures may be installed. Refer to the Acquisitions and Procurement Policy.
* Authentication data – Information Systems must protect authentication data as it is entered including suppressing the display of the password as it is entered, and orienting keyboards away from view.
* Backups – backups protect against accidental or deliberate destruction of data. Refer to the Backup Policy for more information.
* Change – change detection systems (e.g. file-integrity monitoring tools) shall alert personnel to unauthorized modification of critical system files, configuration files, or content files. Such systems shall be configured to perform critical file comparisons at least weekly. Note: For change detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change detection mechanisms such as file-integrity monitoring products usually come preconfigured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by IT security Staff. IT security Staff shall implement a process to respond to any alerts generated by the change detection solution.
* Confidentiality – the requirements for non-disclosure (e.g. confidentiality agreements) reflect ABC Company’s need for to protect data and operational details. Such requirements shall be identified, documented, and reviewed at planned intervals.
* Configurations – Staff must protect data by implementing and maintaining authorized hardware and software configurations. Refer to the Network Configuration Policy, Server Hardening Policy, and Workstation Hardening Policy for more information.
* Denial of Service – a Risk Assessment shall identify Denial of Service (DoS) and Distributed Denial of Service (DDoS) attack threats. A Risk Analysis shall identity the likelihood of the event and impact on the organization. Preventive, detective, and corrective controls shall be identified and implemented as needed.
* Intrusions – intrusion detection systems (IDS) and/or intrusion prevention systems (IPS) shall be used to detect and/or prevent intrusions into the network. All IPS and IPS engines, baselines, and signatures shall be kept up-to-date.
* Malware – security systems must be in place to protect systems against computer "Malware". Refer to the Anti-Malware Policy for more information.
* Monitoring – systems shall monitor all traffic at the perimeter of environments containing sensitive information as well as at critical points in the environment containing sensitive information. Such monitoring systems shall issue alerts to personnel of any suspected compromises.
* Security structure – the security support structure shall maintain a domain for its own execution that protects it from external interference and tampering (e.g. by reading or modifying its code and data structures).
* Services – automated port scans shall be performed on a regular basis against all systems. Alerts shall be issued if unauthorized ports are detected on a system.
* Software – installing unapproved software can cause damage, invalidate warranties, or have other negative consequences. Refer to the Approved Application Policy and the Software Licensing Policy for more information.
* Timeliness – Staff shall act in a timely, coordinated manner to prevent and to respond to breaches of security to help prevent damage. However, if action is taken, it should not jeopardize the security of systems. Refer to the Incident Response Policy for more information.
* Training – ABC Company must establish a computer security awareness and training program. Such a program requires proper planning, implementing, maintaining, and periodic evaluation. Refer to the Security Awareness and Training Policy for more information.
* User interfaces – access to specific functions shall be restricted, never allowing users to request information, functions, or other resources for which they do not have access. Three major user interfaces include menus, database views, and physically constrained user interface (e.g. access card, key, etc.).

Physical security protection

* Environmental conditions – Staff shall minimize costly disruptions caused by data or hardware loss. Refer to the Physical Security Policy to reduce risks related to environmental threats and hazards and opportunities for unauthorized access.
* Display – Staff must be aware of the visibility of data on their computer or handheld device display screens. Staff may need to reposition equipment or furniture to eliminate over-the-shoulder viewing.

For shared environments (multiple entities) the CSO shall:

* Ensure mechanisms protect each entity’s environment and data.
* Ensure that each entity only runs processes that have access to that entity’s data environment.
* Restrict each entity’s access and privileges to its own data environment.
* Ensure logging and audit trails are enabled and are unique to each entity’s environment.
* Enable processes that provide for timely forensic investigation in the event of a compromise to any entity.

E. Incident Response Handling

ABC Company shall establish and maintain a coordination of ABC Company’s response to computerized and electronic communication systems incidents to enable quicker remediation, information gathering and reporting of infrastructure and security related events. Refer to the Incident Response Policy for more information.

F. Emergencies and Disasters

Business continuity planning involves arranging for emergency operations of critical business functions and for resource recovery planning of these functions following a natural or man-made disruption. Refer to the Business Continuity Plan for more information.

# V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to all ABC Company Staff.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT EDM03.02, EDM03.07, APO13.07, APO14.10, DSS05.02, DSS05.07, MEA02.11

GDPR Article 25, 30, 32

HIPAA 164.308(a)(2), 164.308(a)(3)(ii)(B), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(D)

ISO 27001:2013 A.5, A.7.2.2, A.8.1.3, A.8.2.1, A.9-14, A.16-18

NIST SP 800-37 3.4, 3.7

NIST SP 800-53 All XX-1 controls, AC-2, AT-2, AT-3, CP-3, IA-2, IA-8, PL-4, PM-13, PM-29

NIST Cybersecurity Framework ID.AM-5, ID.GV-1, ID.RA-6, PR.AC-1, PR.AT-1, DE.DP-2

PCI 3.7, 4.1, 4.3, 5.1-4, 6.1-2, 6.4, 7.1-3, 8.1-2, 8.4-5, 8.8