Securing Sensitive Information 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

ABC Company has a responsibility to maintain high standards of security for private/non-public electronic information. ABC Company data that is stored on or accessed by computers and other electronic devices must be secured against intentional or unintentional loss of confidentiality, integrity, or availability regardless of location.

# II. Purpose

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

# III. Scope

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

# IV. Policy

Computers and other devices must have an identified local Data Owner who is responsible for the data and can act as a point of contact.

Computers and other devices must be either continuously managed or reviewed on an ongoing basis for appropriate security measures by a full-time information technology professional, such as competent local IT support staff. These reviews must include adherence to baseline security requirements as well as additional strategies for protecting the information.

Units are responsible to have appropriately supervised professional technical support staffing sufficient to maintain information security. The staffing level should be appropriate to the environment considering the amount and type of private information for which they are responsible and the level of risk. Refer to the Staffing Policy for more information.

Computers and other devices must be set up in accordance with applicable ABC Company security guidelines and standards. As received from the vendor, computers and other devices are not configured for security and require initial as well as ongoing review of the configuration and security of the operating system and software.

Security vulnerabilities are regularly found and publicized for software. Regular patching, installation of newer versions, and other maintenance must be performed to protect private data (Patch Management Policy). Automatic settings or centralized updating of security patches is recommended for most desktop computers.

Access to private data must be authenticated (e.g. by using a strong and complex password) with file access privileges differentiated by user. Administrator or root level passwords should be exceptionally strong, since these accounts allow complete control of the system. User accounts with fewer privileges should be used instead of root accounts whenever possible. Periodic review of access is required.

If sent across the Internet (external to the ABC Company's network) or other open networks such as wireless connections, both the authentication data (e.g. user ID and password) and the data itself must be encrypted with strong encryption. Encryption of private data stored on laptop computers or other portable devices is required. An off-site plain-text backup version in a secure location is recommended to protect against lost encryption keys. The ABC Company's wired network is not considered an open network.

Desktop and laptop computers must have anti-virus software or filters installed and updated daily (automatic updates recommended). In addition, other Windows computers, including servers, must have anti-virus software installed and updated daily. (See the Anti-Malware Policy).

Physical access to computers must be restricted as much as possible. Devices not in use for extended periods (e.g. at night and on weekends) must be turned off. Laptops must be physically restrained (e.g. via an anchoring device) at work stations and servers must be in an appropriate and secure physical facility.

Password protected screen saver programs should be used in open locations. Password protected screen savers are required and should be set per the Securing Information Systems Policy.

Host security log files must be configured and reviewed for anomalies. Logs must be of sufficient size to provide useful information in case of a security event (at least 90 days of logs). Refer to the Logging Policy for additional information on log files.

Servers storing private data must be scanned regularly with vulnerability testing software so that corrective actions can be taken as appropriate. Desktop vulnerability scans are regularly sent to the IT technical support staff for review. Servers storing private data are scanned regularly with vulnerability testing software with corrective actions taken as appropriate.

Sensitive Information in databases, logs, data files, backup media, etc. shall be stored securely by means of encryption, masking, truncation, etc. Refer to the Encryption Policy for more information.

Periodic backup copies of software and data must be made, tested, and stored securely. The physical security of the removable media must be maintained and plans made to allow recovery from unexpected problems. Refer to the Backup Policy for more information.

A "secure deletion" program must be used to erase data from hard disks and media prior to transfer or disposal of hardware. Permanent media (e.g., CD's, DVD’s, etc.) must be physically destroyed. Refer to the Disposal Policy for more information.

Services available on computers or other devices must be as limited as much as possible. Web server, ftp server, mail server, peer to peer, and anonymous file sharing software can significantly raise the security risk to private data. Unless a high level of expertise is available and these services are closely monitored at all times, this higher risk software should not be installed.

Training provided by ABC Company on data security practices must be completed for both new and existing employees. Employees that deal with sensitive data may require additional training. Refer to the Security Training Policy for more information.

One or more of the following additional actions should be used to further protect Sensitive Information, depending upon the situation and requirements:

* Limit storage of private data to a hardened file server at the department level.
* Severely restrict the volume and duration of the information stored.
* Move the data to a dedicated computer holding no other applications or data.
* Limit network access to a list of specific machines or devices (access control list).
* Use an internal ABC Company, non-routed IP address or network which prevents any access either to or from the Internet
* Encrypt stored data (with a clear-text version on a removable medium stored in a safe location).
* Sign up for notification of security patch availability from vendors
* Separate any sensitive data from other data and store independently (e.g. on a non-networked device).

ABC Company departments must conduct periodic reviews of information systems in their control that contain private or confidential data.

Each department is required to document the activities they will conduct to review information systems activity. These activities must include:

* Regular review of list of users who have been granted access to systems that contain protected or private information to ensure that only those who need access have access to the systems.
* Periodic review of departmental or unit data security incident trends.
* Periodic review of departmental or unit policies and practices to ensure they address emerging data security trends in the department.
* Document the completion of the periodic reviews described above.
* Periodic review of audit logs.
* Periodic review of user areas to ensure a clear desk for papers and removable storage media and a clear screen. See the Clear Desk Policy for more information.

IT Systems Administrators have the following responsibilities:

* Establish and publish the criteria upon which a server is determined to be a "critical server".
* Periodically review critical server list based on established criteria.
* Perform and review vulnerability scans of critical servers.
* Implement intrusion detection system and review.
* Perform and review ad hoc scans for emerging threats.
* Monitor local data security compliance in the areas for which they are responsible.

A software firewall, hardware firewall, or other network filtering (e.g. port or IP address filtering) technology must be used to protect against Internet threats and to limit network access to devices storing Sensitive Information. Refer to the Firewall Policy for more information.

* Firewalls shall be installed at each Internet connection and between any demilitarized zone (DMZ) and the internal network.
* Firewalls shall be installed and active on mobile devices such as Laptops and similar devices.
* Inbound Internet traffic shall be limited to IP addresses within the DMZ. Firewalls shall not allow direct traffic between the Internet and sensitive data.

Documentation shall be maintained per the Documentation Policy. Firewall documentation shall include:

* Services and ports allowed (inbound and outbound)
* Business need for each service and port
* Information security features to be implemented
* Date of last change

The Chief Security Officer (CSO) shall ensure policies and procedures govern the collection, use, processing, storing, transmitting, and disclosing of Sensitive Information.

* Policies and procedures are clear, reasonable, and protect Sensitive Information.
* Consent is obtained before collecting, using, and disclosing Sensitive Information.
* Sensitive Information is collected in reasonable, appropriate, and lawful ways.

The CSO shall ensure Sensitive Information is:

* Fairly and lawfully processed.
* Processed for limited purposes.
* Adequate, relevant and not excessive.
* Accurate.
* Kept no longer than necessary.
* Processed in accordance with the data’s rights.
* Secure.
* Transferred only to areas with adequate protection.

The CSO shall ensure that data is classified per the Data Classification Policy. Data shall be properly protected according to its classification. Specific security requirements can include:

* Access Controls – see the Access Control Policy
* Awareness and Training – see the Security Awareness and Training Policy and Security Awareness and Training Plan
* Audit and Accountability – see the Audit Policy and Audit Trails Policy
* Configuration Management – see the Security Information Systems Policy, Firewall Policy, Server Hardening Policy, and Router Security Policy
* Identification and Authentication – see the Logical Access Controls Policy
* Incident Response – see the Intrusion Detection Policy, Incident Response Policy, and Incident Response Plan
* Maintenance – see the IT Management Policy
* Media Protection – see the Removable Media Policy and the IT Management Policy
* Personnel Security – see the Personnel Security Policy
* Physical Protection – see the Physical Security Policy and Physical Access Policy
* Risk Assessment – see the Risk Assessment Policy and Risk Management Policy
* Security Audit – see the Security Controls Review Policy, Audit Policy, Audit Trails Policy, and Logging Policy
* System and Communications Protection – see the Security Policy
* System and Information Integrity - see the Audit Trails Policy, Logging Policy, Patch Management Policy, Anti-Malware Policy, Security Policy, and Intrusion Detection Policy

# V. Enforcement

Any Staff member 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 Staff that use ABC Company Information Resources.

**Policy History**

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

**References:**

COBIT EDM03.02, APO01.11, APO13.07, APO14.01-02, APO14.07, APO14.10, MEA03.01

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, .A8.1.3, 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