IT Management 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

This companion policy to the Acceptable Use Policy sets forth department level responsibilities for the operation and maintenance of computers and networks.

# II. Purpose

IT is critical to maintaining ABC Company’s business operations. This policy ensures sufficient resources are allocated to supporting and managing IT and its use within ABC Company.

# III. Scope

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

# IV. Policy

The Chief Security Officer shall be responsible for the development and implementation of security policies and procedures. A formal job description shall identify the responsibilities of the Chief Security Officer and shall reflect the size of the organization, type of information collected, stored, processed, and transmitted, complexity, and technical capabilities of the organization.

Each operating department shall adopt policies governing the use of its IT resources using whatever procedures it normally follows for adopting policies in the department. Such policies shall be consistent with ABC Company’s Acceptable Use Policy and shall include at minimum the following components:

* A statement identifying the kinds of IT resources in the department and establishing general policies for each kind of resources. These policies should require the operating department to identify the persons responsible for each kind of resource, the persons authorized to use the resources, and the uses permitted for the resources. Where appropriate, the policy should cover issues of shared access, resource limitations, and personal use.
* A policy statement regarding mission continuity planning to address system, application, and data backups and procedures for the recovery and restoration of department's mission critical IT resources in the event of loss.

If a department's IT usage does not warrant the development of department specific policies, the department may exercise the option of adopting ABC Company's IT policies as its department level policies.

Departments that do not adopt department policies, and departments that do not have more restrictive policies on personal use of IT resources, shall be deemed to have adopted a policy prohibiting personal use by employees of telephones, pagers, cell phones, computers and other IT resources when such use interferes with the efficient performance of an employee's duties or with the functionality of the department's IT system or when it results in increased operating costs for the department or the ABC Company. Subject to supervisor discretion, incidental personal use of IT resources that does not produce the above effects is authorized. Employees must promptly reimburse the department for any personal use of telephones, cell phones, or other IT resources that result in long distance toll charges or other identifiable increased costs for the department.

A. Responsibility to Maintain Functionality

Each information system at ABC Company is intended to serve some function or set of functions. The department's IT Coordinator shall ensure that the IT systems in the department continue to serve their functions with an appropriate degree of reliability.

The department's IT Coordinator shall facilitate appropriate training and IT knowledge transfer within the department. User training helps employees remain current or expand their technical skills and knowledge of applications. IT Coordinators should direct system users within their respective department to avail themselves of IT training support departments available both within and outside the ABC Company. The department's IT Coordinator is also responsible for communicating important technical information to the users of the department's systems.

B. Security Responsibilities

The IT Director shall establish information security objectives. The objectives shall be consistent with ABC Company’s Security Policy, be measurable (if practical), take into account information security requirements and the results from a recent risk analysis, and be communicated to the appropriate staff.

When planning how to achieve information security objectives, the IT Director shall determine what needs to be done, resources required, responsible parties, timeframes, and how the results will be evaluated.

IT shall provide leadership and direction for the ABC Company's network and systems security. IT has developed and implemented a network architecture that places an emphasis on security. ABC Company's IT security team will develop system security awareness practices, appropriate system safeguards and effective responses to breaches in security within the departments. Security in a networked environment must be a responsibility shared by everyone. A single compromised workstation can be used to attack other systems both within and outside the ABC Company.

IT Coordinators are responsible for establishing, communicating and enforcing department level practices and procedures that promote security. The following areas should be covered:

* Physical security.
* Protection of information, which includes periodic backup and offsite rotation of mission critical systems, applications, and data files.
* Prevention of unauthorized access.
* Detection of security breaches.
* Procedures for reporting security breaches to management or appropriate authority.
* Account auditing which includes the removal of accounts no longer authorized access to the ABC Company's information technology resources. IT Coordinators and technical managers will work with IT security personnel, other system administrators, and law enforcement officials, both inside and outside the ABC Company, to find and correct problems caused on any network or on another system by the use of the system under their control. Where violations of this or any other IT policy come to the IT Coordinator or Technical Manager's attention, they are authorized to take reasonable actions to maintain the security of the system. A user's access privileges may be temporarily suspended if the IT Coordinator or Technical Manager believes it is necessary or appropriate to maintain the integrity of the computer system or network.

The IT Director shall ensure:

* Appropriate contacts with relevant authorities are established and maintained.
* Appropriate contacts with relevant special interest groups (SIG) or specialized security forums and professional associations are established and maintained.
* Information security is addressed in project management regardless of the type of project.

C. Responsibility to Prevent Unauthorized or Inappropriate Access and Disclosure

IT Coordinators are responsible for department level safeguards and procedures that minimize the possibilities of unauthorized access to ABC Company or personal files. As matter of ABC Company policy, no one, including IT Coordinators, Technical Managers and their staff members, may access user files except in the circumstances described below. Even where access is permitted, those who have accessed information must not reveal it to others who are not authorized to receive it. Technical Managers must configure their systems to minimize the possibilities for any unintended disclosure of personal information. In instances where a department does not have a Technical Manager, the IT Coordinator has the responsibility to arrange for the proper configuration of the department's systems.

D. Permissible Access by IT Coordinators, Technical Managers, and Staff

Investigation of System Problems - IT Coordinators, technical managers and their staff members are permitted to access user accounts, files or communications when there is reason to believe that the user is interfering with the performance of the system or network, but only to the extent reasonably necessary to ascertain whether there is a problem and to take corrective measures. In situations in which the IT Coordinator and the Technical Manager have no reason to suspect misconduct on the part of the user, the technical manager or staff member shall advise the user prior to access to the extent reasonably practicable. In situations in which misconduct is suspected, the technical manager or IT Coordinator shall first notify the appropriate authority for investigating disciplinary matters involving the particular user prior to attempting to gain access.

In no case shall a technical manager be restricted from immediately accessing any account, file or communication on a system for which the manager has responsibility, or from taking corrective action, where there is a reasonable belief that a failure to do so will result in loss of system or network stability, substantial damage to the system or network, or liability to the ABC Company.

E. Investigation of Misconduct

As part of an investigation into possible violations of ABC Company rules or policies, or of local state or Federal laws, individual user accounts, files and communications may be accessed as part of the investigation upon a showing that there is reason to believe that the accounts, files or communications contain information relevant to the infractions under investigation. With the exception of authorized IT security personnel, access to a suspect system will not be granted by the IT Coordinator or technical manager without appropriate approvals. In all cases, an authorized IT investigator shall notify the user prior to accessing the user's accounts, files or communications, except where reasonable efforts to contact the user are unsuccessful or upon a showing that prior notification would compromise the investigation. Pending approval of the appropriate administrative head of a department, the authorized investigator may take reasonable steps to ensure that the accounts, files or communications are not altered or destroyed.

F. Where Required by Law

The ABC Company will permit access to individual accounts, files and communications where required to comply with a lawfully issued subpoena, court order, Public Records Act request and other request having the force of law.

G. Access for Coworkers

Each operating department shall develop policies regarding shared access to ABC Company files by coworkers and administrators. In situations in which a co-worker or administrator cannot access files for which they have authorization (because of the absence of an employee on whose workstation they are stored), an IT Coordinator or technical manager, with the approval of the department head, may make such files and only those specific files available to the authorized individual.

H. Responsibility for Policy Adherence

The IT Director shall provide ABC Company-wide leadership over department level adherence to the IT Management Policy. It is expected that departments and offices will become aligned to a department within six months of the ABC Company's adoption of this policy.

Actual department-level policies should be developed and shared with the IT Director within one year of the ABC Company's adoption of the IT Management Policy. Future newly formed departments will have one year to develop a department-level policy for submission to the Office of Information Technology.

IT will monitor department-level progress and will offer assistance to facilitate department formation, department-level policy development and overall compliance to the IT Management Policy. IT Coordinators and technical managers share the responsibility for seeing that ABC Company and local policies governing the use of the system and network are followed. IT Coordinators and technical managers also have the obligation of ensuring that protections for the ABC Company's user community are upheld.

Technical Managers may resolve minor or inadvertent violations. Where more serious violations of such policies have occurred or are suspected, it is the responsibility of the IT Coordinator to assist an investigation by an appropriate authority.

I. System User Responsibilities

Consistent with the ABC Company Acceptable Use Policy, this policy does not relieve ordinary users of personal computers or systems of the responsibility to maintain and protect the integrity and security of information technology resources. If a computer is connected to the ABC Company network, the user is responsible for ensuring that the computer is not used to compromise the security of the network. If the computer contains ABC Company information resources, the user is responsible for data integrity, data backup, physical security of the machine, and for protecting the system from computer viruses and other attacks. In most departments, there are support personnel who will assist the user with these responsibilities.

J. Maintenance of Information Systems

Information Systems shall be properly maintained to sure system integrity, availability, and confidentiality. The IT Director shall ensure that:

* Maintenance activities are properly monitored and managed.
* Controls are implemented to restrict access to tools, techniques, mechanisms, and personnel used to conduct Information System maintenance.
* Data is securely removed from the Information System prior to taking the equipment off-site for maintenance.
* Media containing maintenance, diagnostic, or test programs is checked for malware before the media is used in the Information System.
* Multifactor authentication is employed to protect Information Systems when remote (non-local) sessions are used to maintain equipment. Maintenance sessions are to be terminated when the remote maintenance work is complete.

# 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 Staff members with access to ABC Company’s Information Resources.

**Policy History**

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

**References:**

COBIT APO01.01-03, APO01.05, APO01.07, APO01.11, APO13.07, BAI04.05, DSS04.05

GDPR Article 24, 28, 37

HIPAA 64.308(a)(2), 164.308(b)(4), 164.314(a)(2)(i)

ISO 27001:2013 5, 9, A.5

NIST SP 800-37 3.1, 3.7

NIST SP 800-53 All XX-1 controls, PM-24, SI-5

NIST Cybersecurity Framework ID.GV-1-4, DE.CM-1-6, DE.DP-2

PCI A3.1.2, A3.2.2, A3.3.3