Network Security 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

Networks are a growing and important asset for ABC Company (Company). They provide a critical competitive advantage in the form of information gathering, improved external communications, and increased customer responsiveness. As more and more of our Staff use networks to connect with our customers, service providers, and other key organizations, it is important that Staff understand and agree on the appropriate procedures to protect ABC Company’s assets.

# II. Purpose

This policy outlines the principles, procedures, and guidelines to identify, manage, and maintain security on ABC Company's computer network. It is designed to ensure that our computer network and data is protected from security breaches.

# III. Scope

This policy applies to the Chief Security Officer, department heads, and all Staff that implement and maintain Information Systems.

# IV. Policy

A. Classification

All ABC Company network equipment (e.g. routers, servers, workstations) shall be classified and placed in a network segment appropriate to its level of classification. Access to these segments must be controlled in an appropriate manner. Whenever data travels over a network segmentation of a lower security classification, the data shall be protected in a manner appropriate to its classification level.

All users, hosts, and data shall be classified as security level 1 Public (information intended or required for public release), security level 2 Sensitive (sensitive data that requires additional levels of protection), or security level 3 Confidential (sensitive data that must be protected from unauthorized disclosure or public release). See the Data Classification Policy for more information. All physical network segments, IP subnets and other IP traffic carriers must be classified in the same way. All data travelling on a network must be classified, and all users using network equipment or requesting data over the network must be assigned a level of clearance according to the same system.

It is the function of the person designated as the Resource Owner to have all equipment under his or her control classified. Classification shall be performed in consultation between the Resource Owner, or an assigned representative, and the Chief Security Officer (CSO), but the final decision shall lie with the CSO.

**Classification of Users**

Every user shall be designated as unclassified until the user’s classification is explicitly changed with the written approval of the CSO. When new Staff join ABC Company, a request may be made by the appropriate manager to the CSO for a new level of clearance. It is the responsibility of the manager to justify the requested level of clearance.

Unless there is strong justification, all new Staff shall be cleared for the level ABC Company Only, but only after they have signed acceptance ABC Company policies and non-disclosure forms.

The CSO is responsible for managing and controlling the record of clearance levels for all personnel. It is the responsibility of all Resource Owners and system administrators to determine the security level of a given user before granting that user access to any system.

It is the responsibility of the user to know his or her clearance level and to understand the rights and limitations associated with that clearance.

**Classification of Networks**

The CSO shall classify network segments that constitute part of the ABC Company infrastructure. A complete list of the classifications of all network segments in the ABC Company network and in the ABC Company backbone shall be maintained by the CSO. Classifications for existing ABC Company network segments are as follows:

* Public – ABC Company’s backbone, remote sites, server local area network, portal segment.
* Sensitive – user local area networks.
* Confidential – Server local area network, backup server local area network.

**Classification of Equipment**

The CSO shall assign a classification to all equipment. The CSO shall be responsible for maintaining a complete list of the classifications of all Information Systems in the ABC Company network. Classifications for ABC Company equipment are as follows:

* Public – backbone equipment (e.g. switches, remote access servers) that is not located on premises. Equipment used in the transfer of data to and from the Internet.
* Sensitive – user workstations, print servers, etc.
* Confidential – servers and other hosts used in the management of the ABC Company’s backbone infrastructure and network infrastructure.

**Classification of Data**

For more information see the Data Classification Policy.

B. Network Segmentation

Network segmentation shall be implemented to limit the impact of a network intrusion. Historically, a firewall was implemented at the boundary of an organization’s trusted internal network to the untrusted Internet. Creating one trusted internal network zone wasn't sufficient as it created an environment that allowed an attacker to breach one component and gain widespread access to internal systems. Segmenting a network into smaller groups enhanced security and reduced the impact of an intrusion.

Unless otherwise stated in this Policy, all network segments shall be classified Level 1 - Unclassified. A network segment can only be classified as another security level with approval of the CSO. Applicable Resource Owners shall be notified of changes in classifications.

Network equipment shall not be connected to a network segment that is not of the same security level as the equipment itself. The CSO may choose to segment two networks of the same security level.

C. Trusted Points

Wherever a network segment connects to another network segment with a different security level, the connection between the two networks shall be controlled by an approved trusted point. A trusted point shall include equipment capable of ensuring the security of traffic between two network segments in a manner appropriate to the classification of the networks.

Trusted points shall be under the control of the CSO. Access to any trusted point shall only be granted with the explicit permission of the CSO. The trusted point used to segment two networks shall be appropriate for the network with the higher security level. The CSO shall determine approved connections and related controls between network segments.

Connections into Public segments from

* Public – no controls
* Sensitive – no controls
* Confidential – no controls

Connections into Sensitive segments from

* Public – via a proxy with network level control to and from the proxy, strong user level control
* Sensitive – no controls
* Confidential – no controls

Connections into Confidential segments from

* Public – not permitted
* Sensitive – strong user level controls
* Confidential – no control s

Examples of trusted point technologies include:

* Network level controls – Transmission Control Protocol (TCP) wrappers, allow lists on hosts, router filters, network level firewalls, virtual local area network (V-LAN) switches etc.
* User level controls – application proxies and user level firewalls.
* Strong user level controls – token-based user authentication systems, certificates. Whenever there is a connection that skips over a security level, strong user level control must be used. Even if strong user control is used, a connection may never skip more than one security level.

D. Security Controls

The CSO shall ensure sufficient and effective security controls are implemented and maintained to protect ABC Company’s internal network. For more information see the Information Security Policy.

Access – Information Resources shall be protected against unauthorized access by establishing requirements for the authorization and management of user accounts, providing user authentication, and implementing access controls on Information Resources. Inactivity timeouts and screen savers shall be used to protect against unauthorized access to systems. Accounts shall be locked after a number of failed logon attempts. For more information see the Identification and Authentication Policy and Securing Information Systems Policy.

Anti-virus – desktop and laptop computers must have anti-virus software or filters installed and updated. In addition, workstations and servers must have anti-virus software installed and updated daily. For more information see the Anti-Malware Policy.

Authentication – access to Sensitive Information shall be authenticated (e.g. by using a strong and complex password) with file access privileges differentiated by user. Administrator level passwords shall be exceptionally strong. Wherever possible, user accounts with fewer privileges shall be used instead of administrator accounts. Periodic review of access shall be performed. Password management systems shall be interactive and shall ensure quality passwords. For more information see the Password Policy.

Backups – periodic backup copies of software, data, and system configurations shall be made, tested, and stored in a secure manner. The physical security of the removable media shall be maintained and plans made to allow recovery from unexpected problems. For more information see the Backup Policy.

Communications – processes deny network communications traffic by default (i.e. deny all) and only allow network communications traffic by exception. Communications over unauthorized TCP or UDP ports or application traffic shall be denied to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization’s network boundaries. Security mechanisms prevent remote devices from simultaneously establishing non-remote connections with the Information System while also communicating via some other connection to external networks. Communications with known malicious or unused Internet IP addresses shall be denied and access limited only to trusted and necessary IP address ranges at each of the organization's network boundaries.

Configuration – Information Systems shall be configured in accordance with applicable ABC Company security guidelines and standards. When received from a vendor, computers and other devices may not be configured for security and may require initial as well as ongoing review of the configuration and security of the operating system and software. For more information see the Configuration Management Policy and Network Security Policy.

Design – Information System design and software development principles shall promote effective information security. Processes shall be implemented to monitor, control, and protect Information Systems from information transmitted or received at the external boundaries and key internal boundaries of the Information Systems. An inventory of all of the organization’s network boundaries shall be implemented and maintained.

Disposal – a secure deletion program shall be used to erase data from hard disks and media prior to transfer or disposal of hardware. Permanent media (e.g., CD's, etc.) must be physically destroyed. For more information see the Disposal Policy.

Documentation – network documentation shall be kept up-to-date and be available to authorized personnel. The documentation shall be reviewed annually by a Documentation Analyst to verify it is appropriate, sufficient, and effective at continuing Information Resource availability, confidentiality, and integrity. For more information see the Documentation Policy.

Encryption – cryptographic controls prevent unauthorized disclosure of data during transmission unless otherwise protected by alternative physical safeguards. Authentication data (e.g. user ID and password) and the data itself must use strong encryption. Encryption of Sensitive Information stored on Mobile Computing Devices is required. Encryption is sufficient and effective and according to the classification of the data. Keys are properly managed and maintained. For more information see the Encryption Policy.

Firewall – a software firewall, hardware firewall, or other network filtering technology shall be used to limit network access to the device storing Sensitive Information. For more information see the Firewall Policy.

Incident detection – security policies and procedures identify processes that monitor and analyze security alerts and information, establish, document, and distribute security incident response and escalation procedures, and ensure timely and effective handling of all situations. For more information see the Security Monitoring Policy and Incident Response Policy.

Information Systems – devices must be either continuously managed or reviewed on an ongoing basis for appropriate security measures. These reviews must include adherence to baseline security requirements as well as additional strategies for protecting the information. Devices shall be managed using multi-factor authentication and encrypted sessions. For more information see the Workstation Security Policy, Server Hardening Policy, and Standard Operating Procedure Policy.

Intrusion Detection – Network based Intrusion Detection Systems (IDS) shall be deployed at each of the network’s boundaries. IDS sensors shall examine activity to identify unusual attack mechanisms and detect compromise of these systems.

Logging – Information System log files shall be configured and reviewed for anomalies. Logs must be of sufficient size to provide useful information in the event of a security incident. Logs shall be of sufficient capacity to store at least 90 days of activity. For more information see the Logging Policy.

Owner – Information Systems shall have an identified Resource Owner, such as the principal user of the data or a department supervisor responsible for the data and can act as a point of contact.

Patching – security vulnerabilities are identified on a regular basis. Information Systems shall be patched and updated on a regular and recurring basis. Automatic settings or centralized updating of security patches is recommended for most workstations. For more information see the Patch Management Policy and System Update Policy.

Physical Access – physical access to Information Systems shall be restricted as much as possible. Where applicable, devices not in use for extended periods (e.g. at night and on weekends) must be turned off. Laptops shall be physically restrained (e.g. via an anchoring device) and servers must be in an appropriate and secure physical facility. Risks related to copying, moving, and storing of sensitive information on removable electronic media shall be managed. Information Systems are not to be taken off-site without prior approval from the Data Owner. For more information see the Securing Information Systems Policy, Physical Access Policy, and Physical Security Policy.

Segmentation – networks shall be segmented to protect Information Systems and Sensitive Information. Network segment shall be based upon the classification level of the information stored on the servers. Sensitive Information shall be stored on separate Virtual Local Area Networks (VLANs).

Sensitive Information – one or more of the following shall be used to protect Sensitive Information:

* Maintain an inventory of all Sensitive Information stored, processed, or transmitted by the organization’s technology systems, including those located on-site or at a remote service provider
* Ensure Sensitive Information is stored on hardened servers/devices
* Restrict the volume and duration of Sensitive Information
* Store Sensitive Information on dedicated systems with no other applications or data
* Restrict access to internal systems or devices that contain Sensitive Information
* Encrypt Sensitive Information both in transit and when stored including mobile devices
* Vendor notifications of security updates/patches are implemented in a timely manner
* Automated tools on network perimeters shall monitor for unauthorized transfer of Sensitive Information and blocks such transfers while alerting IT security Staff
* Remove from the network sensitive data or systems not regularly accessed. These systems shall only be used as stand-alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.

Services – Web servers, ftp servers, mail servers, peer-to-peer networks, and anonymous file sharing software can significantly increase the risk to Sensitive Information. As much as possible, services on Information Systems or other devices shall be limited. Unless a high level of expertise is available, and these services shall be closely monitored at all times, higher risk software should not be installed. The IT Department shall be responsible for the installation and maintenance of software. For more information see the Hardware and Software Maintenance Policy.

Third Party Service Providers – risks related to service providers shall be managed and include controls such as remote access is only activated when needed, service provider actions are monitored, and access is immediately terminated when the provider has completed their service. In addition, agreements with service providers shall include appropriate wording related to confidentiality, data breaches, security controls, and audits. For more information see the Third Party Service Providers Policy.

E. Data in Transit

Network technologies are regarded as either "safe" or "unsafe" in their native state (i.e. without any encryption). Data transmitted between any two network-components is considered to be "data in transit". Data in transit also includes all control and management sessions.

All data in transit over an unsafe network segment that has a classification lower than the classification of the data must be protected by strong data encryption. Data in transit over a safe network segment may be encrypted.

Encryption of data in transit may include:

* Network encryption – data is encrypted at the Internet Protocol (IP) layer (e.g. IPsec)
* Session encryption – data is encrypted at a TCP layer (e.g. TLS)
* Message encryption – blocks of data are encrypted before they are sent (e.g. SMIME)
* Data encryption – the entire data package is encrypted before it is transmitted (e.g. file encryption)

For more information see the Encryption Policy.

F. Responsibilities

The CSO shall:

* Approve and maintain a list of all classifications
* Approve ABC Company’s network design and topography
* Control and manage all trusted points
* Ensure security controls are implemented and maintained

Resource Owners and system administrators shall:

* Determine the security level of a given user before granting that user access to any system
* Verify the classification of the equipment they manage
* Verify that the equipment is installed and protected in accordance with its classification

Department heads shall:

* Obtain clearance for Staff in the department
* Clarify the classification of data on systems under the control of the department head
* Clarify the classification of Information Systems under the control of the department head

# 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 the Chief Security Officer, department heads, and all Staff that implement and maintain Information Systems.

**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, 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