Network Configuration 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 Information Systems are provided as a resource for all ABC Company Staff that have access to ABC Company’s network, internal systems, and Internet services. It is important that the infrastructure, which includes cabling and the associated equipment such as routers and switches, continues to develop with sufficient flexibility to meet user demands while at the same time remaining capable of exploiting anticipated developments in networking technology.

# II. Purpose

The purpose of this policy is to establish the rules for the maintenance, expansion and use of the network infrastructure. These rules are necessary to preserve the integrity, availability, and confidentiality of ABC Company information.

# III. Scope

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

# IV. Policy

ABC Company’s IT Department is responsible for managing ABC Company’s network infrastructure and related equipment including firewalls, routers, switches, cabling, servers, etc. The IT Department will manage maintenance and enhancements to this infrastructure.

To provide a consistent ABC Company network infrastructure capable of exploiting new networking developments, all cabling must be installed by the ABC Company IT Department or an approved contractor.

All network connected equipment must be configured to a specification approved by the ABC Company IT Department. In addition, all hardware connected to the ABC Company network is subject to ABC Company IT Department management and monitoring standards.

Changes to the configuration of active network management devices must not be made without the approval of ABC Company IT Department.

The ABC Company network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must be approved by the ABC Company IT Department. The networking addresses for the supported protocols are allocated, registered and managed centrally by ABC Company’s IT Department.

All connections of the network infrastructure to external third-party networks is the responsibility of ABC Company’s IT Department. This includes connections to external telephone networks.

The IT Department must adhere to ABC Company’s Firewall Policy when installing and configuring software or hardware firewalls. The use of departmental firewalls is not permitted without the written authorization from ABC Company’s IT Department.

Firewalls, routers, and switches shall be securely configured. Configuration and security standards for network infrastructure devices including firewalls, routers, switches, virtual environment, servers, workstations, and related components shall be developed and maintained.

Network environments shall be designed and configured to restrict connections between trusted and untrusted networks and reviewed at planned intervals, documenting the business justification for use of all services, protocols, and ports allowed, including rationale or compensating controls implemented for those protocols considered to be insecure. Sub networks shall be implemented and maintained for publicly accessible components that are physically or logically separated by internal networks.

Network architecture diagrams must clearly identify high-risk environments and data flows that may have regulatory compliance impacts. Physical and logical access to diagnostic and configuration ports shall be controlled.

An external and accurate time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate the tracing and reconstitution of activity timelines. Specific legal jurisdictions and orbital storage and relay platforms (US GPS & EU Galileo Satellite Network) may mandate a reference clock that differs in synchronization with the ABC Company’s domicile time reference. In this case, the jurisdiction or platform is treated as an explicitly defined security domain.

Configuration management ensures that protection features are implemented and maintained in the system. Configuration management shall be used to apply a level of discipline and control to the processes of system maintenance and modification.

* Configuration Documentation. Procedures shall be implemented to identify and document the type, model, and brand of system or network component (e.g., a workstation, personal computer, or router), security relevant software product names and version or release numbers, and physical location.
* System Connectivity. Procedures shall be implemented to identify and document system connectivity, including any software used for wireless communication, and any communications media.
* Connection Sensitivity. The sensitivity level of each connection or port controlled by the Security Support Structure shall be documented.

The configuration program shall be documented in a configuration management plan and shall include:

* Formal change control procedures to ensure the review and approval of security relevant hardware and software.
* Procedures for management of all documentation, such as the system security plan and security test plans, used to ensure system security.
* Workable processes to implement, periodically test, and verify the configuration management plan.
* A verification process to provide additional assurance that the configuration management process is working effectively and that changes outside the configuration management process are technically or procedurally not permitted.
* Procedures that monitor growth and traffic patterns to ensure traffic loads can be handled without interruption.

When connecting two or more networks:

* IT security Staff shall review the security attributes of each network (even if the networks are certified at the same protection level) to determine whether the combination of data and/or the combination of users on the connected network requires a higher protection level.
* The interconnected network shall have a controlled interface capable of adjudicating the different security policy implementations of the participating systems or unified networks. An interconnected network also requires certification as a unit.

Systems that process information at different classification levels or require different formal access approvals can be interconnected if:

* Both systems are operating at the same protection level (both systems must be accredited to protect the information being transferred); or
* Both systems are accredited to process the level of information that they will receive, and at least one system is accredited to provide appropriate separation for the information being transferred.

Any information system connected to another system that does not meet the above requirements shall utilize a Controlled Interface that performs the following:

* A communication of lower classification level from within the system perimeter shall be reviewed for classification before being released.
* A classified communication from within the system perimeter shall have the body and attachments of the communication encrypted with the appropriate level of encryption for the information, transmission medium, and target system.
* Communications from outside the system perimeter shall have an authorized user as the addressee (i.e., the communication interface shall notify the user of the communication and forward the communication only on request from the user). If Sensitive Information exists in the communication, it shall be encrypted with the appropriate level of encryption for the information, transmission medium, and target system.

Controlled Interfaces shall filter information in a data stream based on associated security labels for data content:

* There shall be no general users on the Controlled Interface.
* There shall be no user code running on the Controlled Interface.
* The Controlled Interface shall provide a protected conduit for the transfer of user data.
* Communications from outside the perimeter of the system shall be reviewed for viruses and other malicious code.

Controlled Interfaces shall have the following properties:

* Differences. The Controlled Interface shall be implemented to monitor and enforce the protection requirements of the network and to adjudicate the differences in security policies.
* Routing Decisions. The Controlled Interface shall base its routing decisions on information that is supplied or alterable only by the security support structure.
* Restrictive Protection Requirements. The Controlled Interface shall support the protection requirements of the most restrictive of the attached networks or IS.
* User Code. The Controlled Interface shall not run any user code.
* Fail-secure. The Controlled Interface I shall be implemented so that all possible failures shall result in no loss of confidentiality or unacceptable exposure to loss of integrity or availability.
* Communication Limits. The Controlled Interface shall ensure that communication policies and connections that are not explicitly permitted are prohibited.
* In general, such systems have only privileged users; i.e., system administrators and maintainers. The Controlled Interface may have a large number of clients (i.e., individuals who use the CI’s functional capabilities in a severely constrained way). The Controlled Interface application itself will have to provide the more stringent technical protections appropriate for the system’s protection level. Multiple applications do not affect the overall protection provided by the Controlled Interface if each application (and the resources associated with it) is protected from unauthorized access or circumvention from other applications or users.

Each Controlled Interface shall be tested and evaluated to ensure that the Controlled Interface, as implemented, can provide the separation required for the system’s protection level.

# 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 APO01.03, APO03.06, APO12.02, APO12.07, APO13.07, DSS06.08, MEA01.05

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(B), 164.308(a)(2)

ISO 27001:2013 A.8.1.3, .A9.1, A.9.4.1, A.12.1.2

NIST SP 800-37 3.2, 3.4

NIST SP 800-53 3.5, CM-1, CM-3-4, CM-6-7, SA-5

NIST Cybersecurity Framework ID.AM-1-6, ID.BE-4, ID.RA-5, ID.RM-1, DE.CM-1, DE.DP-2

PCI 1.1, A2.1