# Network Security Policy

## Template

This template is part of ISACA's Policy Template Library Toolkit. The policy template should be modified to ensure it conforms to the control posture and reflects the risk tolerance of the specific enterprise environment.

| | |
|---|---|
| **POLICY NAME** | Network Security Policy |
| **DESCRIPTION** | Ensure the company network is protected from security breaches. |
| **OWNER** | Chief information officer (CIO) |
| **EFFECTIVE DATE** | Immediately |
| **REVIEW FREQUENCY** | At least annually |

## INTRODUCTION

### Purpose for Policy

The purpose of this policy is to set out principles for ensuring that Company LLC network security maintains the confidentiality, integrity, and availability (CIA) of its critical infrastructure and information assets, minimizes threats resulting from unauthorized access by users or devices, and restricts authorized user and device connectivity to the company network. It ensures that all employees adhere to network perimeter policies and procedures and that appropriate disciplinary or mitigation actions are taken against those who violate this policy. It also establishes the security responsibilities for network security.

### Scope of Policy

This policy applies to:

a) All employees, contractors, consultants, temporary staff, interns, visitors, and other workers at Company LLC, including all personnel affiliated with third parties and subsidiaries
b) All Company LLC locations where technology resources are located or used
c) All Company LLC technology resources
d) Any information not specifically identified as the property of other parties that is transmitted or stored on Company LLC IT resources (including email, messages, and files)
e) All cloud and on-premise networks, wide area network (WAN) connections to partners, physical and virtual assets, and third-party services that are connected or used by Company LLC or used to access Company LLC technology resources

### Exceptions

Any exceptions to this Policy require submission and approval of appropriate documentation in accordance with the established policy exception process “xxxxx.” Exceptions deemed high risk will be escalated to and reviewed by the “xxxxx Risk Forum” and recorded in the risk register.

## GUIDELINES AND REQUIREMENTS

The list of security measures provided is just one example of how layered security can be implemented. It is important to note that the specific layers and their scope can vary significantly depending on an organization's unique needs, the nature of its digital assets, and industry regulations. In other words, the components of a layered security model should be tailored to the organization's specific risk and requirements, ensuring a customized and robust defense against cyberthreats.

1. **Network Security**
   - Network segmentation
     - Use segmentation to separate specific extranets from vendor, partner, and customer access whenever feasible.
     - Ensure each external network segment allows only specific application traffic to be routed to the specific application hosts and ports that are used to supply services to customers.
   - Traffic flow control, such as documentation of rules, boundary firewalls, secure protocols, and allow-lists
     - Store sensitive information on databases that are not in the demilitarized zone (DMZ) and ensure firewall protection is in place.
   - Perimeter security and DMZ
     - Place systems in separate DMZs based on security level.
     - Restrict connectivity to and from the DMZ and ensure servers accessible from the internet are inside the DMZ.
   - Denial of service (DoS) protection
     - Deploy technology (e.g., routers) with built-in DoS protection or procure these services to detect abnormal traffic flows and redirect the traffic away from the network.

2. **Network Management**
   - Network security monitoring, such as intrusion detection systems (IDSs), intrusion prevention systems (IPSs), security operations centers (SOCs), and administrator access
     - Place an IDS or IPS on all network access points.
     - Deploy and maintain network security appliances that monitor the network or system activities.
     - Produce real-time network traffic logs and retain them according to the Company LLC retention schedule and incident response requirements.
     - Deploy Domain Name System (DNS) servers in a split configuration, where one firewalled DNS server serves public domain information to the outside and does not perform recursive queries, and a second DNS server, in an internal security domain outside the DMZ, performs recursive queries for internal users.

3. **Service and Asset Management**
    - Routers
        - No local user accounts should be configured on the router.
        - Routers and switches must use TACACS+ for all user authentication.
        - The enabled password on the router or switch must be kept in a secure encrypted form.
    - Layer 2 switches
        - Manage the switches in a secure manner. For example, use a Secure Shell (SSH), authentication mechanism, or access list and set privilege levels.
        - Restrict management access to the switch so that untrusted networks are not able to exploit management interfaces and protocols such as Simple Network Management Protocol (SNMP).
        - Always use a dedicated virtual local area network (VLAN) ID for all trunk ports.
    - Content filtering devices
        - Web content filtering policies specify which site categories are blocked on which device groups.
        - Manage web content filtering policies to restrict access to specific parent or child categories as required.
        - Specify a name and description for each policy and select the categories to block (do not select “Uncategorized”).
    - Wireless access points (WAPs)
        - Change the default service set identifier (SSID) of each access point to a unique and nondescript name.
        - Disable SSID broadcasting to prevent unauthorized users from discovering the wireless network.
    - Media Access Control (MAC)
        - Implement media access control (MAC) address filtering to allow only known wireless network interface controllers (NICs) to connect to the network.
    - Voice over Internet Protocol (VoIP)
        - Configure VoIP systems to use secure protocols such as Secure Real-time Transport Protocol (SRTP) or Transport Layer Security (TLS).
        - Implement strong authentication mechanisms for VoIP devices and users, such as two-factor authentication (2FA).
        - Regularly update VoIP systems with the latest security patches and firmware.
    - Remote connections
        - Enforce strong password policies for remote connections, including minimum length, complexity, and expiration requirements.
        - Use multifactor authentication (MFA) to add an extra layer of security for remote connections.
        - Encrypt remote connections using secure protocols such as SSH or virtual private network (VPN).
        - Separate authorization will be required for remote access to the network.
    - Web application firewalls (WAFs)
        - Implement a WAF policy that includes custom and managed rules to control access to web applications.
        - Enable logging diagnostics to monitor and log requests that match WAF rules for analysis and auditing purposes.

    - Define custom response status codes and messages for blocked requests to provide meaningful feedback to users and enhance security awareness.
    - Firewalls, routers, WAPs, and authentication logs must be reviewed regularly for unauthorized traffic.
  - VPNs
    - Only trusted networks and clients should have VPN access.
    - Encryption should be used to minimize the exposure of unauthorized access to confidential files stored on clients connected to the network via a VPN.
    - Unnecessary services on a client-based VPN should be removed to reduce potential exploitation sources.

4. **Network Access Control**
   - There must be a formal, documented user registration and de-registration procedure for access to the network.
   - Access rights for the network must be allocated based on the requirements of a user's job, rather than on a status basis.
   - Users should be sent, and are expected to be familiar with, a terms of use agreement for applications.
   - All users on the network will have their own individual user ID and password.
   - Users are responsible for ensuring their password is kept secret.
   - User access rights, upon notification from departmental managers, will be immediately removed or reviewed for those users who have left the Company LLC or changed jobs.

## ROLES AND RESPONSIBILITIES

1. The Company LLC board, audit and risk committee, and IT committee are ultimately accountable for the management of network security risk and are supported by the senior leadership team (SLT) and the chief operating officer (COO), who oversee network security strategy, funding, and resourcing.

2. The chief information officer (CIO) has the authority to:
   a. Establish network security policies, standards, and guidelines.
   b. Assign management responsibilities for network security.

3. The chief information security officer (CISO) is accountable for:
   a. Management of overall Company LLC network security risk
   b. Providing network security advice and user awareness
   c. Designing and implementing the Company LLC network security strategy
   d. Managing network security incidents

4. Company LLC senior management are accountable for overseeing network security risk within their area of responsibility.

5. Company LLC is responsible for ensuring that appropriate risk assessment(s) are carried out for all the business processes covered by this policy. The risk assessment(s) will identify the appropriate countermeasures necessary to protect against possible breaches of CIA. Internal audit has the ability to undertake an audit of compliance with the policy on request.

6. Information resource owners are responsible for:
    a. Assessing, reporting, and escalating network security risk associated with their IT resources
    b. Assessing and managing network security risk associated with their third-party service providers
    c. Overseeing all access to their IT resources
    d. Management assurance over their network security controls

## CONSEQUENCES OF POLICY VIOLATIONS

Breaches of this policy and/or the Code of Conduct shall be considered grounds for disciplinary action up to and including dismissal.

## QUESTIONS/CONTACT INFORMATION

For questions about the Network Security Policy or any material addressed herein, please email the CIO Policy group (or Information Security or CISO group) at xxxxxxx@CompanyLLC.com.

**DOCUMENT INFORMATION**

| | |
|---|---|
| **Document Location** | Z:\Policies & Procedures\Policies\IT Policies |

**VERSION HISTORY**

| Version | Date | Author | Additional Information |
|---|---|---|---|
| V1.0 | xx/xx/xx | | |
| | | | |

**DOCUMENT REVIEW**

| Version | Date | Reviewed By | Additional Information |
|---|---|---|---|
| V1.0 | | | Approved |
| | | | |
| | | | |
| | | | |