Information Systems Security Policy

Prepared for Laskondo Healthcare

Course: ITEC5010 Security & Enterprise Networks
Capella University
August 6, 2025

Part 1: Implementing a Systems Security Policy

Systems Security Policy Implementation

A robust systems security policy is fundamental to protecting an organization's information assets. For Laskondo Healthcare, a critical component of its systems security policy must be a **Data Classification and Handling Policy**. This policy addresses federal, state, and local cyber defense requirements, particularly those related to Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA).

Data Classification and Handling Policy:

This policy outlines how Laskondo Healthcare classifies its data based on sensitivity and criticality, and specifies the controls required for handling, storing, transmitting, and disposing of each classification.

1. **Data Classification Levels:**
    - **Confidential/PHI:** Data whose unauthorized disclosure could cause severe harm to patients or the organization (e.g., medical records, billing information, social security numbers). This data is subject to HIPAA and state privacy laws.
    - **Internal Use Only:** Data not intended for public release but less sensitive than Confidential/PHI (e.g., internal memos, HR policies).

- **Public:** Data approved for general public consumption (e.g., marketing materials, public announcements).

2. **Handling Requirements:**
    - **Confidential/PHI:**
        - **Encryption:** All PHI must be encrypted at rest (on servers, workstations, and portable devices) and in transit (over networks, including internal and external communications). This directly addresses HIPAA Security Rule requirements for protecting ePHI.
        - **Access Control:** Access must be strictly on a "need-to-know" basis, enforced by strong logical access controls (e.g., multi-factor authentication, role-based access control). This aligns with HIPAA's minimum necessary standard.
        - **Storage:** PHI must be stored on secure, authorized systems with regular backups and disaster recovery plans, meeting HIPAA's availability requirements.
        - **Transmission:** Secure channels (e.g., VPNs, secure email gateways, SFTP) must be used for transmitting PHI, both internally and externally. This is crucial for compliance with federal and state data transmission security standards.
        - **Disposal:** PHI must be securely disposed of (e.g., degaussing, shredding, certified destruction) when no longer needed, in accordance with retention policies and HIPAA's disposal requirements.

- **Internal Use Only:** Requires reasonable access controls and secure storage.
- **Public:** No specific handling requirements beyond organizational branding guidelines.

3. **Compliance and Training:**
    - All employees handling data must undergo mandatory annual training on data classification, HIPAA regulations, and secure data handling practices.
    - Regular audits will be conducted to ensure compliance with this policy and relevant federal, state, and local regulations (e.g., HIPAA, state data breach notification laws).

This policy directly addresses federal requirements like HIPAA by mandating encryption, access controls, and secure handling of PHI. State and local cyber defense requirements are met by ensuring data breach preparedness and secure data transmission practices, which are often reinforced at these levels.

Group Policy Layering Sequence

Group Policy in Windows environments uses a layered approach, and the sequence of application is crucial for effective policy management. The order of precedence is typically: **Local Group Policy Objects (LGPOs) < Site < Domain < Organizational Unit (OU)**. Policies applied at a higher level (e.g., OU) take precedence and overwrite conflicting settings from lower levels (e.g., Local, Site, Domain).

This sequence is designed to provide granular control and flexibility while maintaining a consistent baseline. Here's why this order is significant:

1. **Local Group Policy Objects (LGPOs):** These are applied directly to individual computers. They provide a baseline security configuration for standalone machines or a starting point for domain-joined machines before domain policies are applied.
    - **Why lower precedence?** If LGPOs had higher precedence, a local administrator could easily override critical security policies pushed from the domain, creating security vulnerabilities and inconsistencies across the enterprise.
    - **Example:** A local policy on a workstation might set a screen saver timeout to 30 minutes. However, if the Domain Group Policy sets it to 15 minutes, the Domain policy will override the local one, ensuring all domain-joined workstations adhere to the stricter corporate standard.
2. **Site Group Policy Objects:** These are linked to Active Directory sites, which are defined by network subnets. Policies at this level apply to all computers and users within that specific physical location, regardless of their domain or OU.
    - **Why intermediate precedence?** Site policies are useful for applying settings specific to a geographical location or network segment, such as bandwidth-intensive software deployments or specific firewall rules for a site's network. They need to override domain policies if a site-specific configuration is necessary, but still be overridden by more specific OU policies.

- **Example:** Laskondo Healthcare has three hospitals. A Site policy could be used to enforce specific network access rules for all devices within the "Hospital A" site, which might differ slightly from the general domain policy due to local network infrastructure.

3. **Domain Group Policy Objects:** These are linked to the entire domain and apply to all users and computers within that domain. They establish the foundational security and configuration settings for the entire organization.
    - **Why high precedence over Site/Local but lower than OU?** Domain policies ensure a consistent baseline across the entire enterprise. However, they need to be flexible enough to allow for exceptions or more specific configurations for different departments or groups, which is where OUs come in.
    - **Example:** A Domain policy for Laskondo Healthcare might enforce a universal password complexity requirement for all employees.
4. **Organizational Unit (OU) Group Policy Objects:** These are linked to OUs, which are containers within a domain used to organize users and computers into logical groups (e.g., "Medical Staff," "IT Department," "Finance"). Policies at this level apply only to the objects within that specific OU.
    - **Why highest precedence?** OUs allow for the most granular control. This high precedence enables administrators to apply very specific settings to particular groups of users or computers without affecting the rest of the domain. This is essential for tailoring policies to departmental needs or specific security requirements.

- **Example:** Within Laskondo Healthcare, the "Medical Staff" OU might have a policy that restricts USB device usage to prevent data exfiltration of PHI, overriding a less restrictive domain policy. Similarly, the "IT Department" OU might have policies allowing specific administrative tools that are not permitted for general users. This granular control ensures that policies are applied only where necessary, minimizing disruption while maximizing security for specific roles.

In essence, this layered approach allows for a hierarchical application of policies, moving from general (Local/Domain) to specific (OU), with the more specific policies always taking precedence. This ensures that organizational-wide standards are maintained while allowing for necessary deviations for specific groups or locations.

Significance of a Password Policy

A robust **password policy** is paramount for security because passwords are often the first line of defense against unauthorized access to systems and data. Without strong password policies, even the most sophisticated security controls can be bypassed by simple brute-force attacks or credential stuffing if weak or easily guessable passwords are used. The significance lies in its ability to enforce practices that make passwords difficult to compromise, thereby protecting sensitive information like PHI at Laskondo Healthcare.

Specific Example: Password Minimum Length and Complexity

A highly significant password policy is the enforcement of **minimum length and complexity requirements**. For instance, a policy requiring passwords to be at least **12**

characters long and include a combination of **uppercase letters, lowercase letters, numbers, and special characters**.

Why this is significant for security:

- **Increased Entropy:** Longer passwords with diverse character sets significantly increase the "entropy" (randomness and unpredictability) of the password. This makes it exponentially harder for attackers to guess or crack them using brute-force attacks or dictionary attacks. A 12-character password with mixed characters has a vastly larger keyspace than a 6-character, lowercase-only password.
- **Resistance to Brute-Force Attacks:** Modern computing power can crack short, simple passwords in seconds or minutes. A longer, complex password can take years, decades, or even centuries to crack, making it impractical for attackers.
- **Resistance to Dictionary and Rainbow Table Attacks:** By requiring a mix of character types, the policy renders dictionary attacks (which use common words) and rainbow table attacks (which pre-compute hashes for common passwords) far less effective. Attackers cannot simply use a list of common words; they must account for the varied character sets.

Illustrative Example:

Consider two employees at Laskondo Healthcare:

- **Employee A** uses a password: `laskondo1` (9 characters, lowercase, numbers).

- **Employee B** uses a password: `L@sk0nd0H3alth!` (15 characters, uppercase, lowercase, numbers, special characters).

If Laskondo Healthcare did *not* have a minimum length and complexity policy, Employee A's password `laskondo1` could be easily cracked by an attacker using a common dictionary attack combined with simple number variations. Tools available online can crack such a password in a matter of seconds to minutes. Once cracked, the attacker gains unauthorized access to Employee A's workstation and potentially to patient records (PHI), leading to a HIPAA violation and severe reputational damage.

However, with a policy requiring a minimum of 12 characters and complexity (e.g., `L@sk0nd0H3alth!`), Employee B's password is significantly more resilient. An attacker attempting to brute-force or dictionary-attack this password would face a computational challenge that is practically insurmountable with current technology. This policy directly contributes to the confidentiality and integrity of PHI by making it much harder for unauthorized individuals to gain access through compromised credentials.

Part 2: Network Security Policy for Laskondo Healthcare

Laskondo Healthcare Network Security Policy

Policy Name: Laskondo Healthcare Network Security Policy **Policy ID:** LH-NSP-001 **Version:** 1.0 **Effective Date:** August 6, 2025 **Review Date:** August 6, 2026 **Approved By:** Laskondo Healthcare CIO

1.0 Introduction

Laskondo Healthcare is committed to ensuring the confidentiality, integrity, and availability of its network infrastructure and the sensitive data it transmits, including Protected Health Information (PHI). This Network Security Policy outlines the principles, requirements, and responsibilities for securing all network devices, data in transit, and network access within Laskondo Healthcare's three hospital facilities. This policy is designed to comply with federal regulations such as the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, state data privacy laws, and local cybersecurity guidelines, reflecting modern systems assurance security practices.

2.0 Scope

This policy applies to all network devices (firewalls, routers, switches), network connections, wired and wireless networks, and all individuals (employees, contractors, vendors, volunteers) who access or manage Laskondo Healthcare's network resources. This includes both on-premises infrastructure and any cloud-based network services utilized.

3.0 Policy Objectives

The primary objectives of this Network Security Policy are to:

- Protect the confidentiality, integrity, and availability of all data transmitted over Laskondo Healthcare's networks, especially PHI.
- Prevent unauthorized access to network devices and network resources.

- Ensure network resilience and business continuity.
- Comply with all applicable federal, state, and local laws and regulations governing healthcare data security.
- Establish a framework for secure network operations and incident response.

4.0 Network Device Security

All networking devices (firewalls, routers, switches) must adhere to the following security standards:

4.1 Configuration Management:

- **Secure Baselines:** All network devices must be configured according to secure baseline configurations, hardening guides, and industry best practices (e.g., NIST SP 800-53, CIS Benchmarks).
- **Default Passwords:** All default passwords on network devices must be changed immediately upon installation.
- **Unnecessary Services:** All unnecessary services, ports, and protocols must be disabled.
- **Access Control Lists (ACLs):** ACLs must be implemented on all routers and switches to restrict traffic flow based on the principle of least privilege.
- **Logging:** Devices must be configured to log security-relevant events (e.g., login attempts, configuration changes, traffic anomalies) and forward logs to a centralized Security Information and Event Management (SIEM) system.

4.2 Firmware and Patch Management:

- **Regular Updates:** All network device firmware and operating systems must be regularly updated and patched to address known vulnerabilities. A formal patch management process, as outlined in the organization's Patch Management Policy, must be followed.
- **Vulnerability Scanning:** Regular vulnerability scans of network devices must be conducted to identify and remediate security weaknesses.

4.3 Access Control for Devices:

- **Role-Based Access Control (RBAC):** Access to network devices must be restricted to authorized personnel based on their job function using RBAC.
- **Multi-Factor Authentication (MFA):** MFA must be enabled for all administrative access to network devices.
- **Secure Protocols:** Only secure management protocols (e.g., SSH, HTTPS with strong TLS versions) are permitted for remote access to network devices. Telnet and HTTP are strictly prohibited.
- **Dedicated Management Network:** Where feasible, network device management interfaces should be segregated onto a dedicated, isolated management network.

5.0 Network Segmentation and Zoning

5.1 Network Segmentation:

- The Laskondo Healthcare network must be segmented into logical zones (e.g., patient care, administrative, data center, guest Wi-Fi) to limit the lateral movement of threats and contain breaches.

- Firewalls and VLANs must be used to enforce strict access controls between these segments.

5.2 Demilitarized Zone (DMZ):

- All public-facing servers and services (e.g., patient portals, external vendor connections) must reside in a properly configured DMZ, isolated from the internal network by firewalls.

6.0 Firewall Management

6.1 Firewall Configuration:

- Firewalls (one in each hospital) must be configured to enforce network access policies based on the principle of least privilege, allowing only explicitly authorized traffic.
- Outbound traffic filtering must be implemented to prevent unauthorized data exfiltration.
- Intrusion Detection/Prevention Systems (IDPS) functionalities on firewalls should be enabled and configured to detect and block malicious traffic.

6.2 Firewall Rules Review:

- Firewall rules must be formally reviewed and approved by the IT Security team and relevant stakeholders before implementation.
- Firewall rule sets must be regularly reviewed (at least quarterly) to ensure they are current, necessary, and optimized for security.

7.0 Wireless Network Security

7.1 Secure Configuration:

- All wireless networks must use strong encryption protocols (e.g., WPA3 Enterprise or WPA2 Enterprise with AES). WEP and WPA/WPA2 Personal are prohibited.
- **SSID Broadcasting:** SSID broadcasting should be disabled for internal networks or managed carefully.
- **Guest Networks:** A separate, isolated guest wireless network must be provided for patients and visitors, with no access to the internal production network.

7.2 Authentication:

- Wireless access for employees and authorized devices must utilize strong authentication mechanisms, ideally integrated with the organization's identity management system (e.g., RADIUS with 802.1X).

8.0 Data in Transit Protection

8.1 Encryption:

- All sensitive data, especially PHI, must be encrypted when transmitted across any network, internal or external.
- Secure protocols such as TLS 1.2 or higher for web traffic, SFTP for file transfers, and IPsec VPNs for remote access and site-to-site communication must be used.

- Email containing PHI must be encrypted using approved solutions.

8.2 VPN Usage:

- Remote access to the Laskondo Healthcare network must only be permitted via a secure Virtual Private Network (VPN) connection utilizing strong encryption and multi-factor authentication.

9.0 Monitoring and Logging

9.1 Centralized Logging:

- All network devices must send their logs to a centralized SIEM system for aggregation, correlation, and analysis.
- Logs must be retained for a minimum of one year to support incident investigation and compliance audits, in accordance with regulatory requirements.

9.2 Intrusion Detection and Prevention:

- Network Intrusion Detection Systems (NIDS) and Network Intrusion Prevention Systems (NIPS) must be deployed at strategic points within the network to monitor for malicious activity, unauthorized access attempts, and policy violations.
- Alerts from IDPS systems must be actively monitored by the IT Security team.

10.0 Incident Response

10.1 Network Incident Procedures:

- This policy supports the broader Incident Response Procedures policy by ensuring network-related incidents (e.g., unauthorized access, denial-of-service attacks, malware propagation) are promptly detected, contained, eradicated, recovered from, and post-incident analysis is performed.
- Network logs and monitoring data are critical inputs for incident investigation.

11.0 Policy Enforcement and Review

11.1 Compliance:

- All personnel are required to comply with this Network Security Policy. Non-compliance may result in disciplinary action, up to and including termination of employment or contract.
- Regular audits will be conducted to ensure adherence to this policy.

11.2 Policy Review:

- This policy will be reviewed at least annually, or as necessitated by changes in technology, threats, or regulatory requirements, to ensure its continued effectiveness and relevance.

References

National Institute of Standards and Technology. (2020). NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations.

U.S. Department of Health & Human Services. (2023). HIPAA Security Rule. https://www.hhs.gov/hipaa/for-professionals/security/index.html

Center for Internet Security. (2022). CIS Critical Security Controls v8.