**Week 6:  Capstone Network Security Project**

**Objective:**  Simulate a secure network environment with monitoring and defense.

**Task#04: Write a network security policy for a hypothetical organization, covering acceptable use, passwords, backups, and incident response.**

**Solution:**

**Network Security Policy:**

**Document Version:** 1.0 **Effective Date:** July 22, 2025 **Policy Owner:** IT Security Department **Review Date:** Annually

**1. Introduction**

This Network Security Policy outlines the rules and guidelines for the secure use of network, systems, and data. Its purpose is to protect our information assets, maintain business continuity, and ensure compliance with relevant laws and regulations. All employees, contractors, and third parties with access to our network resources are required to adhere to this policy.

**2. Acceptable Use Policy**

This section defines the permissible use of network resources, including computers, internet access, email, and internal systems.

* **2.1 Purpose of Use:** Network resources are provided primarily for business-related activities. Limited personal use is permitted, provided it does not interfere with job performance, consume excessive resources, or violate any other company policies or legal regulations.
* **2.2 Prohibited Activities:**
  + Accessing, downloading, or distributing illegal, offensive, or inappropriate content (e.g., pornography, hate speech).
  + Engaging in any activity that violates local, national, or international laws (e.g., copyright infringement, fraud).
  + Attempting to bypass security controls, gain unauthorized access to systems, or engage in hacking activities.
  + Installing unauthorized software, applications, or hardware on company devices or networks.
  + Using network resources for commercial purposes unrelated to [Hypothetical Organization Name] without explicit permission.
  + Transmitting chain letters, spam, or engaging in phishing attempts.
  + Introducing malware, viruses, or other malicious code into the network.
* **2.3 Monitoring:** All network activity, including internet usage, email communications, and system access, may be monitored for security, compliance, and performance purposes. Users should have no expectation of privacy when using company resources.

**3. Password Policy**

This policy establishes standards for creating and managing strong passwords to protect user accounts and prevent unauthorized access.

* **3.1 Password Complexity:**
  + Minimum length of 12 characters.
  + Must include a combination of uppercase letters, lowercase letters, numbers, and special characters.
  + Must not contain dictionary words, common phrases, or easily guessable information (e.g., birthdates, names).
* **3.2 Password Uniqueness:** Passwords must not be reused across different systems or services.
* **3.3 Password Rotation:** Passwords must be changed every 90 days. Users will be prompted to change their passwords upon expiration.
* **3.4 Password Confidentiality:** Passwords must be kept confidential and never shared with anyone, including colleagues or IT support staff. Passwords should not be written down or stored in unencrypted formats.
* **3.5 Account Lockout:** Systems will automatically lock accounts after a specified number of failed login attempts (e.g., 5 attempts) to prevent brute-force attacks. Locked accounts will require IT intervention for unlocking.
* **3.6 Multi-Factor Authentication (MFA):** MFA is mandatory for all remote access to the company network and for access to critical systems and sensitive data.

**4. Data Backup Policy**

This policy ensures the regular backup and recovery of critical company data to minimize data loss and support business continuity in the event of system failures, data corruption, or disasters.

* **4.1 Scope:** This policy applies to all critical business data stored on company servers, network drives, and designated cloud services. Employees are responsible for storing critical work-related data on approved network locations that are subject to backup.
* **4.2 Backup Frequency:**
  + **Critical Data (e.g., databases, financial records):** Daily incremental backups, with weekly full backups.
  + **User Data (e.g., network shares, designated cloud sync folders):** Nightly incremental backups.
  + **System Configurations:** Weekly backups of critical system configurations (e.g., servers, network devices).
* **4.3 Backup Retention:**
  + Daily backups: Retained for 7 days.
  + Weekly backups: Retained for 4 weeks.
  + Monthly backups: Retained for 12 months.
  + Annual backups: Retained for 7 years.
* **4.4 Offsite Storage:** Critical backups must be stored offsite in a secure location, physically separated from the primary data center, to protect against site-specific disasters.
* **4.5 Backup Verification & Testing:** Backup integrity will be verified regularly. Full data restoration tests will be conducted at least annually to ensure data recoverability and the effectiveness of the backup process.

**5. Incident Response Policy**

This policy outlines the procedures for identifying, responding to, containing, eradicating, recovering from, and learning from cybersecurity incidents.

* **5.1 Incident Definition:** A security incident is any event that compromises the confidentiality, integrity, or availability of information systems or data, or violates security policies. Examples include malware infections, unauthorized access, data breaches, and denial-of-service attacks.
* **5.2 Reporting Incidents:** All employees are required to immediately report any suspected or confirmed security incidents to the IT Security Department or their direct manager.
* **5.3 Incident Response Team (IRT):** An Incident Response Team will be designated with clear roles and responsibilities for handling security incidents.
* **5.4 Response Phases:**
  + **Preparation:** Maintaining tools, training staff, and developing response plans.
  + **Identification:** Detecting and confirming a security incident.
  + **Containment:** Limiting the scope and impact of the incident (e.g., isolating affected systems).
  + **Eradication:** Removing the root cause of the incident (e.g., removing malware, patching vulnerabilities).
  + **Recovery:** Restoring affected systems and data to normal operation.
  + **Post-Incident Analysis:** Reviewing the incident to identify lessons learned and improve future security measures.
* **5.5 Communication:** Clear communication protocols will be established for internal and external stakeholders during an incident, including legal counsel and affected parties (if a data breach occurs).
* **5.6 Forensic Analysis:** In the event of a significant incident, forensic analysis will be conducted to determine the cause, scope, and impact, and to gather evidence for potential legal action.

**6. Policy Enforcement**

Violation of this Network Security Policy may result in disciplinary action, up to and including termination of employment, and may also lead to legal prosecution.