Cyber Security Policy

1. Password Management

- **Policy:**
    - Use **long, complex passwords** with a mix of uppercase, lowercase, numbers, and special symbols.
    - Change passwords at **random intervals** or in response to any virus/security incident.
    - Password change frequency:
        - **Minimum:** 1 month
        - **Maximum:** 6 months
- **Logic:**
  Long, complex passwords significantly increase the time required for brute-force attacks, making unauthorized access difficult. Regular password updates ensure that even compromised credentials become obsolete. Enforcing changes after incidents ensures immediate risk reduction.

---

2. Software Download Policy

- **Policy:**
    1. **Do not download unapproved software** on company systems.
    2. Pre-install ad blockers on all browsers.
    3. Avoid clicking on suspicious links or downloading files from untrusted websites.
- **If an unknown file is downloaded:**
    1. **Immediately disconnect the computer** from the network to prevent further spread.
    2. Report the issue to the IT department immediately.
    3. **No punishment** will be issued to encourage quick reporting.
    4. **Complete a questionnaire** detailing:
        - Purpose of the download.
        - Reason for visiting the website.
        - Website details (URL).
- **Logic:**
  Malicious software often disguises itself as legitimate downloads. Restricting unauthorized downloads prevents accidental infections. The questionnaire helps IT understand user intent and identify potential patterns or gaps in awareness to improve

future training.

---

3. Email Security

- **Policy:**
    - **Report all unexpected or suspicious emails** to the IT department.
    - IT will evaluate the source of suspicious emails and **block the sender** if deemed a threat.
- **Logic:**
  Phishing emails are among the most common methods attackers use to infiltrate systems. Reporting and blocking suspicious sources helps stop these attacks before they escalate. Encouraging users to flag concerns fosters vigilance.

---

4. Detection

- **Monitoring and Detection Tools:**
    - Use security monitoring systems to detect suspicious activity such as:
        - **Login attempts** from unauthorized or unusual locations.
        - **Anomalous behavior**, such as sudden spikes in network traffic, unexpected file downloads, or unapproved software installation.
        - **Unauthorized changes** to system configurations or file access permissions.
    - Implement Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) tools to monitor and flag potential threats in real-time.
- **Indicators of Compromise (IoCs):**
    - Multiple failed login attempts.
    - Files being accessed, encrypted, or deleted unexpectedly.
    - Unexpected system slowdown or abnormal application behavior.
    - Reports of suspicious emails, links, or files.
- **Logic:** Early detection is critical to mitigating damage. Monitoring systems, combined with real-time alerts, allow IT teams to identify and respond to threats before they escalate. Behavioral analysis helps uncover potential breaches not immediately visible through traditional logs.

---

5. Incident Response Plan

Containment

- **Steps to Contain the Incident:**

    1. **Identify the infected systems** and affected devices.
    2. **Disconnect infected systems** from the network to prevent lateral movement or further spread.
    3. Isolate backups to ensure they remain untouched by malicious software.
- **Logic:**
  Containment limits the spread of malware or unauthorized access across systems. Disconnecting affected systems and isolating backups ensures business continuity and protects unaffected devices.

Eradication

- **Steps to Remove the Threat:**

    1. Identify and **remove the malicious software** (e.g., virus, ransomware, spyware) from affected systems.
    2. Investigate and **fix vulnerabilities** that allowed the breach (e.g., outdated software, weak passwords).
- **Logic:**
  Simply removing the malware without addressing root vulnerabilities leaves the system open to reinfection. Fixing gaps ensures a more secure environment moving forward.

Recovery

- **Steps to Restore Normal Operations:**

    1. **Restore systems** from clean backups or newly built systems.
    2. **Verify system integrity** to confirm no malware or vulnerabilities remain.
    3. Monitor systems for a period to ensure no residual issues persist.
    4. Conduct a **post-incident review** to analyze:
        - Cause of the incident.
        - Steps taken to contain and eradicate the threat.
        - Recommended measures to prevent future occurrences.
- **Logic:**
  Recovery ensures minimal downtime and restores trust in system safety. Post-incident analysis helps improve the security posture by identifying and addressing underlying risks.

---

6. Preventive Measures

- **Install Ad Blockers:** To reduce exposure to malicious ads and websites.
- **Network Monitoring:** Implement tools to detect unauthorized logins or anomalous behavior.
- **Training & Awareness:** Conduct regular training sessions to teach staff how to identify suspicious activity, phishing emails, and proper download procedures.
- **Patch Management:** Keep all systems, software, and security tools up to date to close vulnerabilities.
- **Logic:**
  Prevention is always more cost-effective than incident response. Training users and maintaining up-to-date software minimizes the likelihood of breaches occurring in the first place.

---

7. User Responsibilities

- Follow all password, email, and download policies.
- Immediately report any suspicious activity or breaches to IT.
- Complete post-incident questionnaires honestly for review purposes.
- **Logic:**
  Clear expectations for users encourage accountability and timely reporting, which are essential to security efforts.