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.

- **Legal Alignment:**
    - Under **GDPR** (Article 32), organizations must implement measures to ensure data security, including protection against unauthorized access. Regular password updates and strong password policies align with these requirements.
    - **HIPAA** requires covered entities to have safeguards for electronic protected health information (ePHI), including authentication and password management practices.

---

2. Software Download Policy

- **Policy:**
    - **Do not download unapproved software** on company systems.
    - Pre-install ad blockers on all browsers.
    - Avoid clicking on suspicious links or downloading files from untrusted websites.
- **If an unknown file is downloaded:**
    - **Immediately disconnect the computer** from the network to prevent further spread.
    - Report the issue to the IT department immediately.
    - **No punishment** will be issued to encourage quick reporting.

    - **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.

- **Legal Alignment:**

    - Under **CCPA**, businesses must take measures to prevent unauthorized access to consumer data. Avoiding malicious downloads helps mitigate risks that could lead to data breaches.
    - **GDPR** (Recital 39) emphasizes safeguarding against malware that could expose personal data.

---

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.

- **Legal Alignment:**

    - **HIPAA** requires safeguards to protect ePHI, including email communication practices to avoid unauthorized disclosures.
    - **GDPR** requires organizations to mitigate risks arising from phishing emails that could compromise personal data.

---

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.

- **Ethical Consideration:**

    - Transparency in detection practices aligns with ethical principles of **accountability** and **trust**. Users should be informed about monitoring activities to ensure privacy rights are respected.

---

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:**

    - **Restore systems** from clean backups or newly built systems.
    - **Verify system integrity** to confirm no malware or vulnerabilities remain.
    - Monitor systems for a period to ensure no residual issues persist.
    - 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.

- **Legal Alignment:**

    - **GDPR** (Article 33) requires organizations to notify supervisory authorities and affected individuals within 72 hours of a data breach. The recovery plan must ensure breaches are handled transparently and promptly.
    - **CCPA** mandates timely notifications to California residents whose personal information may have been compromised.
- **Ethical Consideration:**

    - Transparency during recovery fosters trust with stakeholders and ensures ethical accountability. Communicating breaches promptly upholds the principle of **honesty**.

---

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.

- **Legal Alignment:**

    - Under **HIPAA**, regular training is required to ensure employees can safeguard ePHI effectively.
    - **GDPR** (Article 39) emphasizes regular staff training as part of an organization's compliance measures.

---

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.

- **Ethical Consideration:**

    - Encouraging user transparency in reporting aligns with the principles of **responsibility** and ensures a culture of trust and collaboration.

bf

Decrypted text

Hello you can read this text

Encrypted Text

E3M9cw7UfSMr/ulrBixrRWOZUFCblijOiSJoQWH0Nao=

Secret Code

SuperSecret