Cybersecurity Incident Response Plan and Security Policy

1. Incident Response Plan

1.1 Detection of Security Incidents To detect security incidents effectively, we employ a combination of automated and manual detection methods. One key method is the use of **Intrusion Detection Systems (IDS)** and **Security Information and Event Management (SIEM)** tools. These systems monitor network traffic and log data continuously for suspicious activity, alerting administrators when anomalies are detected.

Additionally, we encourage employees to report unusual behavior or system errors through an internal ticketing system to help identify potential insider threats or social engineering attacks.

1.2 Containment Strategy The primary strategy for containing a security incident is **network segmentation and isolation**. Once an incident is detected:

- The affected system(s) are immediately disconnected from the network.
- Access controls are updated to prevent the spread of the threat.
- Backups are verified and secured.
- Incident Response Team (IRT) is activated to assess and coordinate containment actions.

1.3 Eradication and Recovery Steps

- **Eradication**:
    - Identify the root cause of the incident.
    - Remove malware or unauthorized software.
    - Patch vulnerabilities exploited during the incident.
- **Recovery**:
    - Restore systems from clean backups.
    - Monitor restored systems for signs of residual threats.
    - Reconnect systems to the production environment in phases.
    - Notify affected stakeholders and resume normal operations.

1.4 Example Cyber Attack: Ransomware Ransomware is a type of malware that encrypts files and demands payment for the decryption key. In the event of a ransomware attack:

- Isolate infected systems.

- Inform law enforcement and internal stakeholders.
- Avoid paying the ransom as it does not guarantee data recovery.
- Use clean backups to restore data after ensuring all malware is removed.

2. Comprehensive Security Policy

2.1 Security Rules and Guidelines

1. **Password Policy**: Employees must use complex passwords with at least 12 characters, including uppercase, lowercase, numbers, and special characters. Passwords must be changed every 90 days.
2. **Access Control**: Access to sensitive systems is granted based on the principle of least privilege. Multi-factor authentication (MFA) is required for all administrative accounts.
3. **Acceptable Use Policy**: Employees are prohibited from installing unauthorized software or accessing non-work-related websites on company systems. All internet activity is monitored.

2.2 CIA Triad Alignment

- **Confidentiality**: Encryption protocols, access control mechanisms, and data classification ensure only authorized personnel can access sensitive data.
- **Integrity**: File integrity monitoring and secure coding practices are used to ensure data remains accurate and unaltered.
- **Availability**: Regular system backups, disaster recovery plans, and redundant network infrastructure ensure continuous access to systems and data.

3. Legal and Ethical Compliance

3.1 Relevant Laws and Regulations

1. **General Data Protection Regulation (GDPR)**: This law mandates strict data protection and privacy requirements for organizations handling personal data of EU citizens. Key requirements include consent for data processing, breach notification within 72 hours, and rights to data access and erasure.
2. **Health Insurance Portability and Accountability Act (HIPAA)**: Applies to healthcare organizations, requiring them to protect sensitive patient health information. Includes requirements for administrative, physical, and technical safeguards.

3.2 Ethical Consideration An important ethical principle in cybersecurity is **transparency**. Organizations must inform users when their data is compromised and take responsibility for lapses in security.

3.3 Compliance in the Plan This incident response plan ensures legal and ethical compliance by:

- Including breach notification procedures aligned with GDPR and HIPAA.
- Enforcing strict access controls and data encryption to prevent unauthorized access.
- Promoting transparency through prompt communication with stakeholders and affected users during an incident.

4. Encryption and Hashing Demonstration

4.1 AES Encryption/Decryption Example

- **Plain Text**: My name is sosa
- **Encryption Method**: AES (Advanced Encryption Standard)
- **Key Used**: sosasosasosasosa (128-bit key)
- **Mode**: CBC (Cipher Block Chaining)
- **Encrypted Text**: Lpyu3EoeAsagJFbArHDpdw==
- **Decrypted Text**: My name is sosa

This example shows how AES can ensure confidentiality by encrypting sensitive data and securely decrypting it when needed.

4.2 Hashing Examples Using the text "My name is sosa", here are the hash values generated:

Uppercase 'M':

- **MD5 Hash**: a152b492b3811db76013724ae3e0be06
- **SHA1 Hash**: 44bdd308fd2533ff81d6795bbb1fc0645d6311f7

Lowercase 'm':

- **MD5 Hash**: c6e677cecace250d10a466d1f6cd9f2a
- **SHA1 Hash**: 70ee9fc7db1476bd64bb6d26d4f7d7ab226de6be

This demonstrates that hashing is highly sensitive to even minor changes in input and is effective for verifying data integrity.

Conclusion This integrated report provides a holistic cybersecurity strategy that combines detection, response, and recovery from security incidents. It outlines clear policies that support the CIA triad, ensures compliance with major legal frameworks, demonstrates secure encryption and hashing methods, and upholds ethical standards. The organization is committed to proactive cybersecurity practices and continuous improvement.