Incident response plan

1. **Detection Methods**
    - **Network Monitoring**
        - Implement network monitoring to detect unauthorized access and abnormal traffic patterns.
        - Isolate sensitive payment data and monitor access attempts.
        - Regularly review logs that may indicate a breach.
    - **Security Information and Event Management**
        - Implement a system to analyze logs from various sources.
        - Real-time analysis of security events to identify potential breaches.
    - **Endpoint Detection and Response**
        - Tools will be installed on all systems and employee devices to monitor for malicious activity.
        - Continuous monitoring for malware or unauthorized access attempts.
        - Automated incident response actions, such as quarantining affected devices.

2. **Incident Classification**
    - **Low (Level 1)**
        - Minor issues that can be resolved quickly (e.g., a minor IT glitch, a non-critical equipment failure).
        - If malware is involved, quarantine infected files or isolate the impacted device.
        - Remove the threat (e.g., delete malicious emails, run antivirus scans).
        - Ensure affected systems are functioning normally and restore any lost data if necessary.
    - **Medium (Level 2)**
        - Incidents that have a moderate impact on the organization, requiring a coordinated response and potentially affecting multiple users or systems.
        - Infections on non-critical systems, moderate data leaks, or compromised user accounts without sensitive access.
        - Remove malware, reset passwords, and apply security patches. Conduct forensic analysis to determine the attack vector
    - **High (Level 3)**
        - incidents that pose significant risk to the organization, potentially leading to substantial financial loss, data breaches, or regulatory consequences.
        - Isolate affected systems from the rest of the network to prevent lateral movement by the attacker.
        - Identify and eliminate malware or unauthorized software installed during the attack.
        - Apply security patches and updates to affected systems to close vulnerabilities that were exploited.

3. Target Incident Response

Scenario: Target data breach of 2013

1. **Preparation**
    - Create and regularly update incident response policies and playbooks tailored to different types of breaches.
    - Regularly train staff on incident response procedures and conduct tabletop exercises to test readiness.
2. **Identification**
    - Use intrusion detection systems (IDS) and security information and event management (SIEM) tools to monitor for unusual activity.
    - Collect logs and alerts from firewalls, antivirus software, and intrusion detection systems to identify suspicious activities.
    - Assess the extent of the breach, identifying affected systems, networks, and data types.
3. **Containment**
    - Implement temporary fixes to stop the breach from spreading while preparing for more permanent solutions
    - Isolate affected systems to prevent further unauthorized access. Disconnect compromised devices from the network.
4. **Eradication**
    - Clean and secure affected systems by removing any malware or unauthorized access points.
5. **Recovery**
    - Restore systems from clean backups and ensure they are free from vulnerabilities.
    - Continuously monitor restored systems.

Key Security Rules/Guidelines

1. **Access Control Policy**
    - Only authorized personnel should have access to sensitive information.
    - Implement role-based access control (RBAC) to limit access to data based on user roles.
    - Regularly review access rights and promptly revoke access for employees who leave the organization.
2. **Data Encryption Policy**
    - All sensitive data must be encrypted both in transit and at rest using industry-standard encryption protocols.
    - Ensure that encryption keys are stored securely and managed appropriately.
    - Conduct regular audits to verify compliance with encryption protocols.
3. **Security Awareness Training**
    - All employees must undergo cybersecurity awareness training annually.
    - Training should cover phishing detection, secure password practices, and the importance of reporting security incidents.
    - Provide regular updates on emerging threats and organizational security policies.

CIA

1. Confidentiality

- Ensures that sensitive information is only accessible to authorized individuals or systems.
    - Use encryption to protect data at rest and in transit.
    - Implement access controls and authentication mechanisms.
    - Conduct regular training on data privacy for employees.

2. Integrity

- Ensures that information is accurate, consistent, and has not been tampered with or altered by unauthorized individuals.
    - Utilize checksums and hashes to verify data integrity.
    - Implement version control and auditing processes.
    - Use access controls to prevent unauthorized modifications.

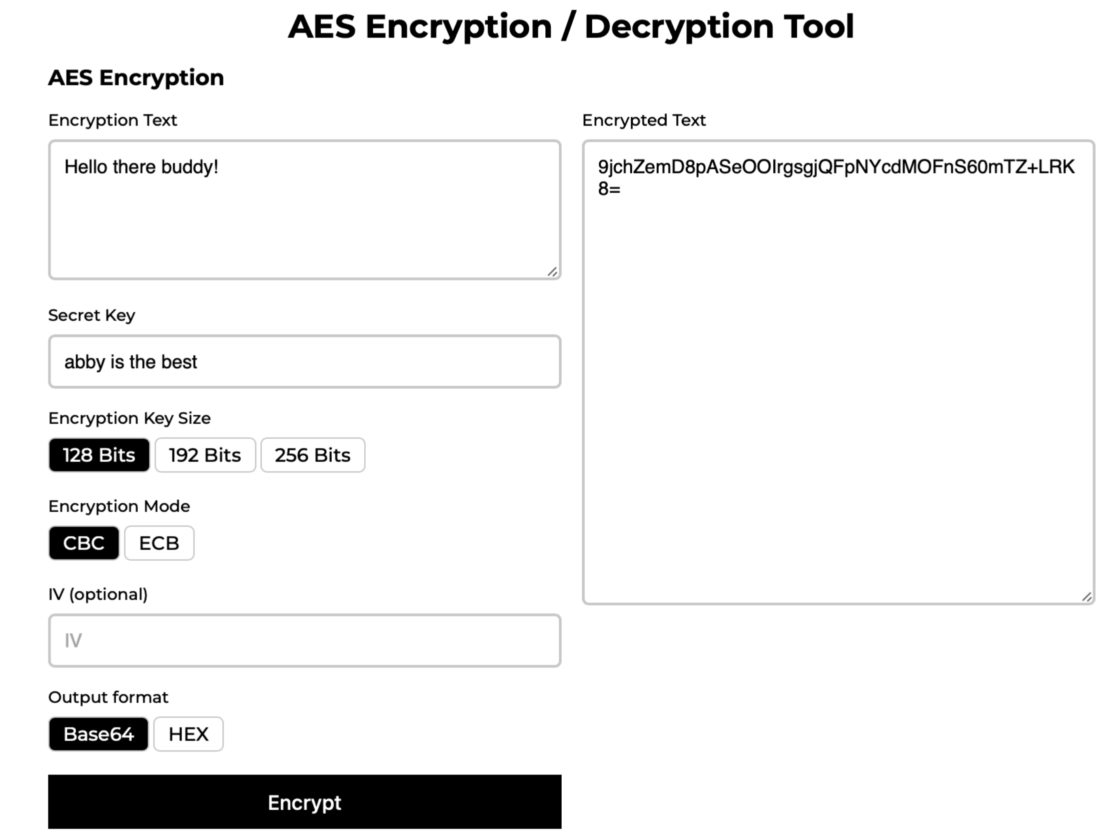
3. Availability

- Ensures that information and resources are accessible to authorized users when needed.
    - Implement redundancy and failover systems to maintain service during outages.
    - Regularly back up data and test recovery procedures.

- ○ Monitor system performance to identify and resolve potential issues proactively.

Encryption Techniques

- AES
  - Encrypted Text: 9jchZemD8pASeOOIrgsgjQFpNYcdMOFnS60mTZ+LRK8=



AES Encryption / Decryption Tool

AES Encryption

Encryption Text: Hello there buddy!

Secret Key: abby is the best

Encryption Key Size: 128 Bits

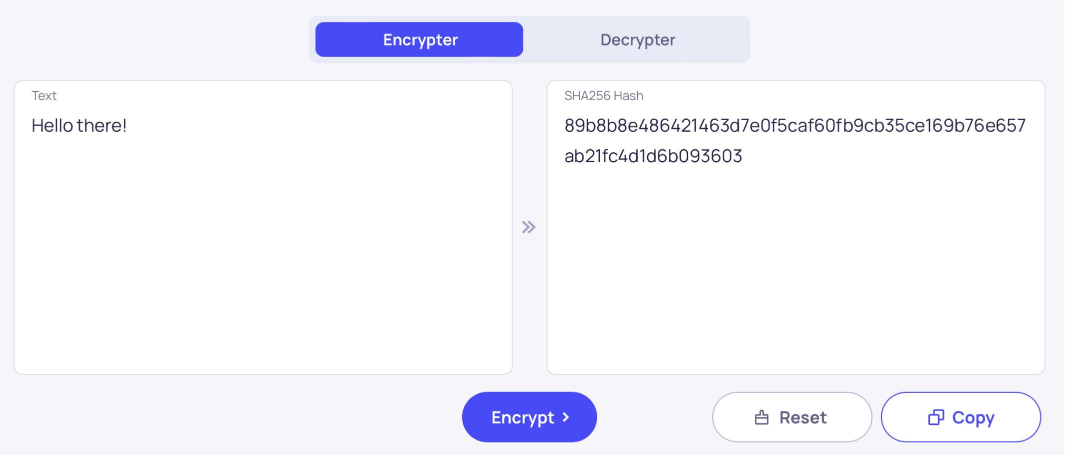
Encryption Mode: CBC

IV (optional): IV

Output format: Base64

Encrypted Text: 9jchZemD8pASeOOIrgsgjQFpNYcdMOFnS60mTZ+LRK8=

- SHA256
  - Encrypted Text: 89b8b8e486421463d7e0f5caf60fb9cb35ce169b76e657ab21fc4d1d6b093603



Text: Hello there!

SHA256 Hash: 89b8b8e486421463d7e0f5caf60fb9cb35ce169b76e657ab21fc4d1d6b093603

Legal and Ethical Compliance in the Incident Response Plan

Relevant Laws and Regulations

1. **General Data Protection Regulation (GDPR)**
   - The GDPR is a comprehensive data protection law in the European Union that regulates how organizations handle personal data. Key provisions include the requirement for organizations to report data breaches within 72 hours and the obligation to implement adequate security measures to protect personal data.
   - **Compliance in Incident Response Plan:** The incident response plan includes a procedure for timely breach notification to affected individuals and regulatory authorities, ensuring that response actions are in line with GDPR requirements.
2. **Health Insurance Portability and Accountability Act (HIPAA)**
   - HIPAA is a U.S. law that mandates the protection of patient health information. It requires covered entities to implement security measures to safeguard electronic protected health information (ePHI) and to have breach notification protocols in place.
   - **Compliance in Incident Response Plan:** The plan incorporates specific steps for identifying and managing breaches involving ePHI, including notifying affected individuals and regulatory bodies as required by HIPAA.

Ethical Considerations

- **Respect for Privacy and Confidentiality**
  - An ethical consideration in incident response is the obligation to respect the privacy and confidentiality of affected individuals. This includes handling personal data responsibly and transparently throughout the incident management process.
  - **Upholding Ethical Principles:** The incident response plan emphasizes the need for secure data handling practices and ensures that any communication regarding breaches is conducted with transparency, minimizing harm to affected parties. Additionally, it includes measures to avoid unnecessary exposure of sensitive information during investigations.

Alignment with Legal and Ethical Standards

- **Timely Communication and Transparency**
  - The incident response plan ensures that legal requirements for breach notifications are met while also committing to transparent communication with stakeholders, upholding ethical standards.
- **Documentation and Accountability**
  - Detailed documentation of incident response actions is required to demonstrate compliance with laws like GDPR and HIPAA. This also fosters accountability within the organization, ensuring that all actions taken during an incident are justifiable and in line with ethical practices.
- **Training and Awareness**

- Regular training on legal obligations and ethical considerations is incorporated into the security awareness program, ensuring that all employees are aware of their responsibilities and the importance of compliance in incident response.