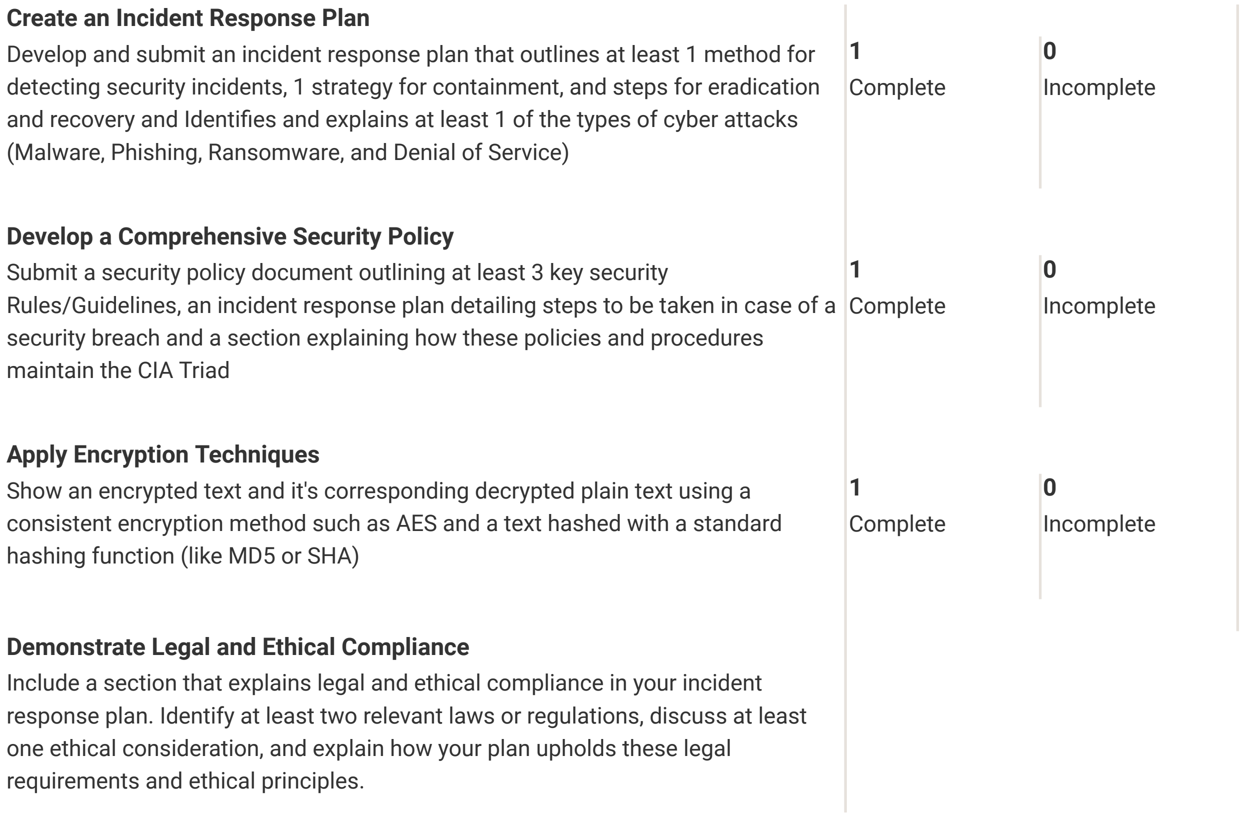


Create an Incident Response Plan Develop and submit an incident response plan that outlines at least 1 method for detecting security incidents, 1 strategy for containment, and steps for eradication and recovery and Identifies and explains at least 1 of the types of cyber attacks (Malware, Phishing, Ransomware, and Denial of Service)	**1** Complete	**0** Incomplete
Develop a Comprehensive Security Policy Submit a security policy document outlining at least 3 key security Rules/Guidelines, an incident response plan detailing steps to be taken in case of a security breach and a section explaining how these policies and procedures maintain the CIA Triad	**1** Complete	**0** Incomplete
Apply Encryption Techniques Show an encrypted text and it's corresponding decrypted plain text using a consistent encryption method such as AES and a text hashed with a standard hashing function (like MD5 or SHA)	**1** Complete	**0** Incomplete
Demonstrate Legal and Ethical Compliance Include a section that explains legal and ethical compliance in your incident response plan. Identify at least two relevant laws or regulations, discuss at least one ethical consideration, and explain how your plan upholds these legal requirements and ethical principles.		

<u>Incident Responce Plan</u>

- Log Monitoring and Analysis: Set up log monitoring for all systems, including databases, applications, and network devices. Log analysis tools should aggregate data to detect unusual activities like multiple failed login attempts, sudden file deletions, or changes in system configurations.
- Immediate Isolation of Affected Systems: Upon detecting a breach, isolate affected systems or networks to prevent the spread of the incident. For example, if a server shows signs of malware, disconnect it from the main network to stop lateral movement.
- Malware Scanning and Removal: Use advanced antivirus and anti-malware tools to scan and remove any malicious software from compromised systems. This includes scanning for rootkits, trojans, and viruses that may have been embedded in the system.
- Restore from Backups: Use the latest secure backups from several sources such as online databases, in house backups, and dedicated “cold” storages to restore data and system configurations. This will help bring systems back online while ensuring data integrity.

Cyber Attack Type - Ransomware

- Detection and Isolation: Immediately isolate the infected system from the network immediately. Prevent further encryption of files by disconnecting affected systems.
- Data Restoration and Decryption: Avoid paying ransoms by restoring files and mission critical data from secure backups that were proactively made

Security Policy at Facebook

1. Protecting Customer & Employee Data

- Data Encryption: Encrypt sensitive data both at rest and in transit. Use AES-256 encryption for stored data and TLS for data transmitted over networks to ensure data confidentiality.
- Access Control Management: Implement strict access control policies to restrict data access to authorized personnel only. For example, customer information should only be accessible to employees whose roles require it, following the principle of least privilege.
- Data Masking: For added security, mask personally identifiable information (PII) in user records, ensuring unauthorized users cannot view sensitive data.

2. Required Security Policies for Employees

- Password Policy: Enforce a password policy that requires employees to use strong passwords (minimum of 12 characters with a mix of letters, numbers, and symbols) and change them every 90 days.
- Multi-Factor Authentication (MFA): Require MFA for all employees accessing internal systems and sensitive applications to add an extra layer of security.
- Phishing and Security Training: Conduct mandatory security awareness training to educate employees about phishing attacks, social engineering tactics, and best practices for maintaining cybersecurity hygiene. Employees should learn to identify suspicious emails and report them to the security team immediately.

3. Maintaining the CIA Triad (Confidentiality, Integrity, Availability)

- Confidentiality: Ensure that sensitive customer and employee data remains secure through encryption, access control, and employee training. Only authorized individuals should have access to critical information, reducing the risk of data leaks.
- Integrity: Implement checksums and hashing mechanisms to verify the integrity of data during storage and transmission. Use version control to prevent unauthorized changes to system configurations or customer records.
- Availability: Ensure systems and data are available to authorized users by implementing redundant systems, regular backups, and disaster recovery plans. Regular system

maintenance and patching should be done to prevent downtime due to security vulnerabilities.

Legal and Ethical Compliance

1. Relevant Laws and Regulations

- General Data Protection Regulation (GDPR): As a company operating internationally, Facebook must comply with GDPR, which mandates that companies protect the personal data and privacy of EU citizens. This includes requirements for data minimization, lawful processing of data, and the rights of individuals to access and control their personal information.
- California Consumer Privacy Act (CCPA): Facebook must also comply with the CCPA, which grants California residents rights over their personal information. This includes the right to know what data is being collected, the right to delete personal information, and the right to opt-out of data sales.

These regulations set strict standards for data security and incident response, requiring organizations to notify affected users and regulatory bodies promptly in the event of a breach.

2. Ethical Consideration

- Transparency and User Trust: It’s essential for Facebook to maintain transparency with its users regarding data collection, usage, and security practices. In the event of a security breach, Facebook has an ethical responsibility to inform affected users honestly and in a timely manner. Upholding transparency builds trust and shows commitment to ethical practices in data management.

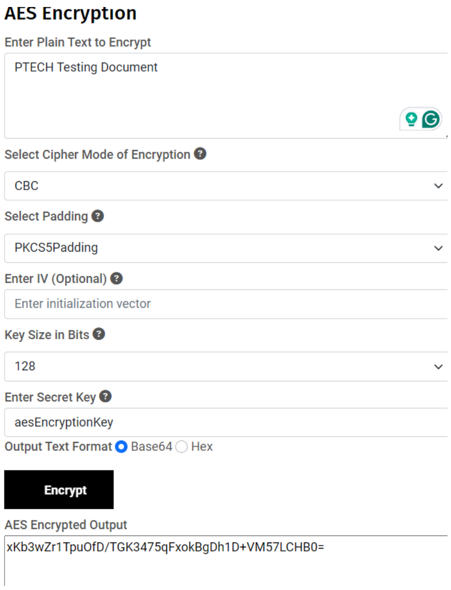
Encryption standards

AES Encryption

Unencrypted Text - PTECH Testing Document

Encrypted Text using AES & Secret Key (Base64 - aesEncryptionKey) - “xKb3wZr1TpuOfD/TGK3475qFxokBgDh1D+VM57LCHB0=”

Encrypter Image —>



AES Encryption

Enter Plain Text to Encrypt

PTECH Testing Document

Select Cipher Mode of Encryption

CBC

Select Padding

PKCS5Padding

Enter IV (Optional)

Enter initialization vector

Key Size in Bits

128

Enter Secret Key

aesEncryptionKey

Output Text Format ● Base64 ○ Hex

AES Encrypted Output

xKb3wZr1TpuOfD/TGK3475qFxokBgDh1D+VM57LCHB0=

Text Hashing

- String - PTECH Test
- MD5 Hash - 6aed5cdf8327eac532e44aa50bfcbb6a
- SHA1 Hash - 444285311cf6c3310a86dbbbe40b2dfe8fcfc20a