Incident Response Plan	
1. Detection Method	
Method: Intrusion Detection System (IDS)	
Description: Implement an IDS to monitor network traffic for suspicious activity and anomalies that may indicate a security breach. This system will alert the security team in real-time, allowing for rapid response to potential incidents.	
2. Containment Strategy	
Strategy: Network Segmentation	
Description: Upon detection of a security incident, immediately isolate affected systems by segmenting the network to prevent the spread of the attack. This can include disabling affected user accounts, restricting access to sensitive data, and utilizing firewalls to block malicious traffic.	
3. Eradication and Recovery Steps	
Eradication Steps:	
Identify and eliminate the root cause of the incident, such as malware or unauthorized access points.	
Apply necessary patches and updates to systems.	
Recovery Steps:	
Restore systems from clean backups.	
Monitor the environment for any signs of persistent threats.	
Review and revise security measures to prevent future incidents.	
4. Cyber Attack Explanation	
Type of Attack: Ransomware	

Description: Ransomware is a type of malicious software that encrypts the victim’s files, rendering them inaccessible until a ransom is paid. It typically spreads through phishing emails, malicious attachments, or exploit kits.	
Comprehensive Security Policy	
1. Key Security Rules/Guidelines	
Access Control: Implement the principle of least privilege, ensuring users only have access to the data and systems necessary for their job functions.	
Data Encryption: Mandate the use of encryption for sensitive data at rest and in transit to protect against unauthorized access.	
Regular Updates: Require regular updates and patching of all software and systems to mitigate vulnerabilities.	
2. Incident Response Steps	
Preparation: Establish an incident response team and develop training programs.	
Identification: Utilize monitoring tools to detect incidents.	
Containment: Isolate affected systems to prevent spread.	
Eradication: Remove the threat and any vulnerabilities.	
Recovery: Restore systems and data from backups.	
Lessons Learned: Conduct a post-incident review to improve response strategies.	

3. CIA Triad Maintenance	
Confidentiality: By enforcing access controls and encryption, sensitive information remains accessible only to authorized users.	
Integrity: Regular updates and incident reviews help maintain data integrity, preventing unauthorized modifications.	
Availability: Incident response procedures ensure that systems can be restored quickly, minimizing downtime and maintaining availability.	
Encryption Techniques	
Example of AES Encryption	
Plain Text: "Hello, World!"	
Encrypted Text (AES): 2e7d2c03a9507ae265ecf5b535228ea1	
Decrypted Plain Text: "Hello, World!"	
Example of Hashing with SHA-256	
Plain Text: "Hello, World!"	
Hashed Text (SHA-256): a591a6d40bf420404a011733cfb7b190d62c65bf0bcda190eb1b2e1e8cda7c88	
Legal and Ethical Compliance	
Relevant Laws/Regulations	
General Data Protection Regulation (GDPR): Mandates strict data protection and privacy standards for individuals in the EU.	

Health Insurance Portability and Accountability Act (HIPAA): Establishes national standards for protecting sensitive patient information.	
Ethical Consideration	
Data Privacy: Ethical handling of user data is critical to maintain trust and comply with legal requirements. Organizations must ensure transparent data collection and usage policies.	
Upholding Legal and Ethical Principles	
The Incident Response Plan incorporates legal compliance by ensuring data protection measures align with GDPR and HIPAA requirements. Ethical considerations are upheld through transparent communication with stakeholders regarding data handling and incident management.	