# Incident Response Plan (IRP)

## Purpose

The purpose of this Incident Response Plan (IRP) is to establish a clear and organized approach for detecting, containing, eradicating, and recovering from cybersecurity incidents. This plan ensures that incidents are handled efficiently to minimize impact and restore normal operations.

## 1. Detection Method: Intrusion Detection System (IDS)

### Overview:

An Intrusion Detection System (IDS) monitors network traffic for suspicious activity and known threats, generating alerts when it detects potential security incidents.

### Detection Process:

- Deploy IDS solutions across critical network points.
- Continuously monitor logs and alerts generated by IDS.
- Automatically notify the security team if unusual patterns or known signatures of attacks are detected.
- Verify alerts with manual investigation when necessary to reduce false positives.

## 2. Containment Strategy: Network Segmentation and Isolation

### Immediate Containment Steps:

- Identify the affected systems and network segments.
- Disconnect compromised devices from the network to prevent the attack from spreading.
- Block malicious IP addresses or domains using firewalls.
- Apply temporary network access controls to quarantine affected areas while maintaining critical operations elsewhere.

### Purpose:

Rapid containment limits the attack's spread, protects sensitive data, and gives the security team time to assess the damage without further exposure.

# 3. Eradication and Recovery Steps

## Eradication:

- Identify all components of the incident (e.g., malware binaries, malicious user accounts, unauthorized processes).
- Remove malware, delete malicious files, and close any exploited vulnerabilities.
- Apply security patches and software updates to prevent reinfection.
- Conduct a thorough system scan to ensure no remnants of the attack remain.

## Recovery:

- Restore affected systems from clean backups.
- Monitor restored systems closely for any signs of lingering issues.
- Gradually reintroduce systems back into the production environment.
- Conduct a full system and network audit post-recovery to verify integrity.

# 4. Type of Cyber Attack: Ransomware

## What is Ransomware?

Ransomware is a type of malicious software that encrypts a victim's files, making them inaccessible. The attacker then demands payment (often in cryptocurrency) for the decryption key needed to restore access.

## How Ransomware Works:

- Typically delivered through phishing emails, malicious downloads, or exploiting vulnerabilities.
- Once executed, it silently encrypts files on the victim's system.
- A ransom note is displayed, providing instructions on how to pay and threatening permanent loss of data if demands are not met.

### Preventive Measures:

- Regularly back up critical data and store backups offline.
- Train employees on recognizing phishing attempts.
- Implement strong endpoint protection and keep all systems updated.
- Restrict user permissions to limit malware spread.

# Conclusion

This Incident Response Plan provides a structured approach to detecting, containing, eradicating, and recovering from security incidents, specifically focusing on threats like ransomware. Timely and coordinated action following this plan helps minimize the damage caused by cyber attacks and ensures the organization's resilience.