**Ransomware Incident Response Plan**

# Introduction to the NIST Cybersecurity Framework

The **NIST Cybersecurity Framework** (**CSF**) is a set of voluntary guidelines designed to help organizations assess and improve their ability to prevent, detect, and respond to cybersecurity risks. Developed by the U.S. [National Institute of Standards and Technology](https://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology) (NIST), the framework was initially published in 2014 for critical infrastructure sectors but has since been widely adopted across various industries, including government and private enterprises globally. The framework integrates existing standards, guidelines, and best practices to provide a structured approach to cybersecurity risk management.

# Incident Summary:

# TechCo Under Ransomware Attack

TechCo, a fictional company providing cloud services, suffered a ransomware attack initiated via a phishing email containing a malicious attachment. Once opened, the ransomware infected several critical systems, including the file server, customer database, and internal backups. The attackers demanded a ransom of 50 Bitcoins (over $1,000,000) with a 72-hour deadline.

# Identify

- Critical assets affected: File server, customer database, and internal backup systems.

- Identified vulnerabilities of phishing awareness, poor network segmentation, insecure backup strategy, and inadequate email filtering.

- Lack of data protection security in the rules on the EDR / XDR

# Protect

- Implement security awareness training and phishing simulations.

- Deploy email security gateways and endpoint protection platforms.

- Enforce network segmentation and access controls (least privilege, MFA).

- Maintain regular offline or immutable backups.

# Detect

- Utilize Security Information and Event Management (SIEM) systems and Endpoint Detection and Response or Extended Detection and Respond (EDR/XDR).

- Deploy Intrusion Detection Systems (IDS) and anomaly detection tools.

- Establish automated alert protocols and measures to continuous network monitoring and block automatically incidents if needed.

# Respond

- Isolate infected systems and initiate forensic analysis.

- Notify stakeholders and assemble the incident response team.

- Rotate credentials, disable compromised accounts, and report to legal entities.

- Define internal/external communication strategy and document incident handling.

# Recover

- Restore data from clean, offline backups and re-imaging affected systems.

- Conduct validation tests before reintegration.

- Ensure phased recovery and maintain business continuity through alternate operations.

- Communicate status updates to clients and partners.

# Continuous Improvement

- Conduct post-incident reviews and lessons-learned sessions.

- Evaluate incident metrics (time to detect, respond, recover).

- Refine playbooks, training programs, and update policies.

- Run periodic tests and exercises to improve.