

Ransomware Response Documentation Form

Incident Summary

Date & Time of Incident

Reported By

Affected Location(s) / Department(s)

Short Incident Description

Detection & Initial Response

How was the Ransomware Detected?

Initial Actions Taken

System Impact

Systems/Devices Affected

Type of Data/Files Impacted

Evidence of Encryption/Ransom Note

Containment & Eradication

Containment Steps Taken

Eradication Steps Taken

Recovery

Recovery Process

Was Backup Used?

Systems Restored

Communication

Internal Notification & Escalation

External Notification (e.g., authorities, clients)

Lessons Learned & Recommendations

Root Cause Analysis

Recommendations / Improvements