Ransomware Incident Documentation

Incident Identification

Date & Time of Discovery

Reporter Name/Contact

Affected System(s)

Location (Physical/Network)

Incident Details

Incident Description

Ransom Note Details (if any)

Ransomware Family/Type (if known)

Initial Entry Point (if known)

Impact Assessment

Systems/Services Impacted

Data Encrypted or Exfiltrated

Business Impact

Response Actions

Actions Taken

Incident Handlers Involved

External Parties Notified

Lessons Learned / Follow-Up

Root Cause Analysis

Recommendations