Malware Infection Incident Report

Date/Time of Incident:

Reported By:

Department/Team:

Incident Details

Affected System(s):

System Owner/User:

Description of Incident:

Indicators of Compromise (e.g., popups, slow performance, unknown processes):

Time and Method of Detection:

Scope of Infection (number and names of affected devices, if known):

Type of Malware (if identified):

Response Actions

Immediate Actions Taken:

Systems Isolated/Disconnected:

Remediation Steps Performed:

Was the incident escalated? If so, to whom:

Impact Assessment

Business Impact:

Data Compromised or Exfiltrated:

Estimated Downtime:

Lessons Learned & Recommendations

Root Cause Analysis:

Preventive Measures Recommended:

Additional Comments: