

Malware Outbreak Incident Log Template

General Information

Incident Title

Date & Time Detected

Incident Handler / Team

Reported By

Location / Department

Affected Systems

System Name / ID	User	IP Address	Operating System	Status	Date Isolated

Incident Details

Description of Malware & Impact

Indicators of Compromise

Actions Taken

Communication Log

Resolution & Recovery Steps

Lessons Learned / Recommendations

Closure

Date & Time Closed

Incident Handler Signature
