Incident Report

Incident ID- 001   Date -/-/-   Time- :   Reported By-   Incident Type- i.e. Malware

Detection and initial response

Detection method	*How the incident was identified i.e. using a SIEM alert, IDS/IDS, user report*
Affected Systems	*Impacted devices, networks, or accounts*
Initial Actions Taken	*Immediate containment or mitigation steps*

Incident Details

This section would go into detail about what happened, how it was identified, IoCs such as suspicious IPs, file hashes, or registry changes, as well as looking the into attack vector and vulnerability it exploited

Action

This section describes remediative actions including details on containment, eradication steps, recovery measures, and restoring systems

Impact Assessment

Details of scope including who/ what was affected and the impact it had if any on business operations

Future Recommendations and Preventative Measures

This section describes lessons learned and what preventative measures should now be put in place for the future, this could include changes to policies, or device configurations

Supporting Evidence- This section would show any relevant screenshots of things like logs, or suspicious emails