Incident ID:

Date of Report: 1/25/25

Reported by: Levi Ingle, Documenter, Dunwoody College of Technology

Incident Severity Level: High, Med, Low

Incident Description:

The incident was a \_\_\_\_\_\_\_ attack. The incident was detected by our team while we were scanning the \_\_\_\_\_\_. The following were the affected systems and data:

Timeline of Events:

Date/time: Initial detection, Name/Team

Date/time: Initial response, Name/Team

Date/time: Escalation/remediation steps, Name/Team

Actions Taken:

Detection and Analysis: Summarize how the incident was identified and verified.

Containment: We mitigated the risk and limited it to as few components of the network as possible.

Eradication: Patched vulnerabilities and restored the network or data to full potential.

Recovery: Explain how we restored and verified the restoration of the system.