Network Intrusion Investigation Report

1. General Information

Report ID:

Date of Report:

Prepared By:

Reviewed By:

2. Executive Summary

3. Incident Overview

Incident Date & Time:

Detection Method:

Location / Affected Systems:

Incident Description:

4. Technical Details

Indicators of Compromise (IoCs):

Attack Vector:

TTPs (Tactics, Techniques & Procedures):

Evidence Collected:

5. Impact Assessment

Data Affected:

Business Impact:

6. Response Actions

Immediate Actions Taken:

Remediation Steps:

Current Status:

7. Recommendations

8. Appendices