IT Security Incident Investigation Report

1. General Information

Report Number:

Date & Time of Report:

Reporter Name & Contact:

Investigator(s):

2. Incident Description

Describe the incident, including date & time of occurrence, type of incident, systems/users affected, and how the inci

3. Initial Assessment

Summarize initial impact, severity assessment, and containment steps if any.

4. Investigation Details

Detail the investigative actions taken, evidence collected, analysis performed, and findings.

5. Root Cause Analysis

Provide analysis of the underlying causes of the incident.

6. Remediation & Recovery Actions

List immediate and long-term steps taken to address the incident, restore systems, and prevent recurrence.

7. Lessons Learned & Recommendations

Describe lessons learned and suggestions for policy, process, or technical improvements.

8. Report Closure

Closure Date:
Investigator Signature:
Reviewed By: