Cybersecurity Incident Response Report

1. Executive Summary

Summary of the Incident

Date and Time of Detection

2. Incident Description

Reported By

Affected Systems/Assets

Incident Type

Incident Description

3. Impact Assessment

Scope of Impact

Data/Information Affected

Business Impact

4. Incident Response Actions

Immediate Actions Taken

Containment Measures

Eradication Steps

Recovery Steps

5. Root Cause Analysis

Cause of the Incident

How Was the Incident Detected?

6. Lessons Learned & Recommendations

Lessons Learned

Recommendations

7. Appendices

Evidence Collected

Incident Timeline

Contacts & Investigators