Incident Response Plan

Company: Atharva

Industry Sector: mmcoe

Infrastructure Type: mmcoe

Number of Endpoints: 4

Compliance Standards: HIPAA

CSIRT Model: sarang

Incident Commander: A

Audience Roles: mine

1. Executive Summary

2. Introduction

This Incident Response Plan (IRP) outlines procedures and responsibilities for responding to cybersecurity incidents in Atharva.

The document is aligned with frameworks such as NIST 800-61 and ISO 27035.

3. Detection Capabilities

EDR/SIEM Used:

Detection Tools: xyz

Top Threats: virus

Response Playbooks: yes

4. Roles and Responsibilities

Incident Commander: A

Audience: mine

The organization has a fully staffed internal CSIRT and SOC to ensure 24/7 incident detection and response capabilities.

5. Containment and Eradication

Containment Strategies: yes

6. Recovery Procedures

Critical Systems:

Backup System: atg

7. Compliance and Disclosure

Disclosure Time: tr

8. Threat-Specific Response

9. Appendices

Appendix A — Situation Update Log

Date/Time	Update	Submitted By
[timestamp]	[details]	[person]

Appendix B — Resolution Action Plan

Step #	Action	Assigned To	Due Date	Status
1	[Action]	[Person]	[Date]	[Open/Closed]

Appendix C — Assets & Contacts

Asset	Location	Owner	Criticality
[Asset]	[Location]	[Name]	[High/Medium/Low]