Incident Response Plan

1. Organization Overview

Company Name: Atharva

Industry Sector: N/A

Number of Endpoints: N/A

Infrastructure Type: N/A

Critical Systems: N/A

Backup System: N/A

EDR/SIEM Used: N/A

2. Roles and Responsibilities

Incident Commander: N/A

Audience Roles: N/A

3. Compliance Obligations

As per GDPR, any breach must be reported to the Data Protection Authority within 72 hours of discovery.

4. CSIRT Model

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

5. Containment Strategy

6. Detection and Threat Response

Detection Tools: N/A

Disclosure Time: N/A

Top Threats: Phishing

Phishing response includes resetting credentials, alerting affected users, and updating email filtering rules.

7. Response Playbooks

N/A

Appendix A – Situation Update Template

Date of Entry:	
Time of Entry:	
Author:	
Date and Time Incident Detected:	
Current Status:	New / In Progress / Resolved
Incident Type:	
Incident Classification:	Incident / Significant / Emergency
Scope:	
Impact:	
Severity:	

Notifications:	
Additional Notes:	
Contact for Incident Manager:	
Next Update Due:	

Appendix B – Resolution Action Plan

Date/Time	Category	Action	Owner	Status

Appendix C – Evidence Register

Collection Details	Collected By	Item Info	Storage Location	Access Log

Appendix D – Assets and Key Contacts

Site Information

- IP Subnet
- DHCP Scope
- Core Router IP
- DNS Servers (Internal) – Logs & Locations
- DNS Name – Logs & Location
- Secondary DNS Name (External)

Internet & Communication

- ISP IP & Connection Details

- Network Provider Details
- VoIP / PABX Systems – IPs & Ranges
- 3G/4G & Satellite Services
- Single Point of Failure – Communications Infrastructure

Firewall & Security

- Firewall Software/Hardware
- Wired/Wireless Networks
- SPoF – Firewall Infrastructure

Remote Access

- Remote Methods – Logs & Locations
- SPoF – Remote Access Infrastructure

Network Infrastructure

- Wired/Wireless Network Switches – Firmware/Logs
- SPoF Analysis

ICS / SCADA Systems

- SCADA PLC RTU – Logs & Firmware
- Authentication Controls
- Process Flow Diagrams
- Configuration Backup Schedule
- Alarms & Thresholds

Data Backup

- Backup Software
- Backup Locations & Restoration Timeframes
- Data Retention Requirements
- Disaster Recovery Plan
- High Availability Identified? (Yes/No)
- Required Uptime (%)
- Return to Operation (Hrs)

Redundant Power Supply / UPS

- UPS Hardware & Locations
- Battery Capacity & Run Time
- Connected Devices

Redundant Power / Generator

- Generator Hardware & Location
- Fixed or Portable
- Capacity (KVA)
- Fuel Type / Capacity (L)
- Fuel Consumption (L/Hr)
- On-Site Fuel Storage & Locations
- Fuel Supply Arrangements
- Failover / Restoration Procedures

Administration Systems

- Web Proxy – Logs & Locations
- Domain Controller – Logs & Locations
- Web Server – Logs & Locations
- Server OS Environments – Logs
- Virtual Server Host – Logs & Config

Email and Database Systems

- Email Server – Logs & Locations
- Production Database – Logs
- Test Database – Logs

Cloud Service Providers

- Hosted Service Providers & SLAs

Staff Devices

- Client OS – Logs & Locations
- Hardware Model & Manufacturer

Appendix E – Glossary

- **Incident:** A violation or threat of security policy.
- **CSIRT:** Computer Security Incident Response Team.
- **EDR:** Endpoint Detection and Response.
- **SIEM:** Security Information and Event Management.
- **Threat:** Potential cause of an adverse event.
- **Vulnerability:** Weakness subject to exploitation.
- **IDS:** Intrusion Detection System.
- **IPS:** Intrusion Prevention System.
- **Phishing:** A social engineering attack to steal credentials.
- **Ransomware:** Malware that encrypts data for ransom.
- **DDoS:** Distributed Denial of Service attack.
- **MSSP:** Managed Security Services Provider.