

## Document 1

### Southstar Tech Solutions

### Cybersecurity Incident Response Standard Operating Procedure (SOP)

**Version:** 1.0

**Effective Date:** January 2026

**Owner:** Security Operations Center (SOC)

---

#### 1. Purpose

This SOP defines the standardized process for detecting, analyzing, containing, eradicating, and recovering from cybersecurity incidents at **Southstar Tech Solutions**. The objective is to minimize business impact and ensure rapid restoration of services.

---

#### 2. Scope

This procedure applies to:

- All Southstar Tech employees
  - Contractors and third-party vendors
  - All company-managed devices and cloud systems
  - On-premise and cloud infrastructure
- 

#### 3. Roles and Responsibilities

##### Security Operations Center (SOC)

- Monitor security alerts in the SIEM (Splunk)
- Investigate suspected incidents
- Lead containment and mitigation efforts

##### IT Operations Team

- Implement system isolation and restoration
- Apply patches and security configurations

### Compliance Officer

- Ensure regulatory reporting requirements are met
- Review post-incident documentation

### Department Managers

- Coordinate communication with affected teams
  - Approve recovery timelines
- 

## 4. Incident Classification

### Severity Description

Low      Minor issue, no business impact

Medium   Limited system disruption

High      Critical system compromise

Critical   Major data breach or outage

---

## 5. Incident Response Procedure

### Step 1: Detection and Reporting

- Monitor alerts from Splunk SIEM.
- Log incident in ServiceNow within **15 minutes** of detection.

### Step 2: Triage and Classification

- Analyze the alert.
- Assign severity level.
- Escalate High/Critical incidents to SOC Manager immediately.

### Step 3: Containment

- Disconnect affected systems from network.
- Block malicious IPs at firewall.

- Disable compromised accounts.

#### **Step 4: Mitigation and Eradication**

- Remove malicious software or files.
- Apply system patches and updates.
- Validate that threat has been neutralized.

#### **Step 5: Recovery**

- Restore systems from Veeam backups.
- Reconnect systems after security validation.
- Monitor for recurrence.

#### **Step 6: Post-Incident Reporting**

- Complete Incident Report within 24 hours.
  - Submit to Compliance and IT leadership.
  - Conduct root cause analysis.
- 

### **6. Communication Protocol**

- SOC Manager informs stakeholders within 1 hour of critical incidents.
  - External communication must be approved by Compliance.
- 

### **7. Compliance Alignment**

This SOP aligns with:

- NIST Cybersecurity Framework (Detect, Respond, Recover)
  - ISO 27001 Incident Management guidelines
- 

### **8. Tools Used**

<b>Tool</b>	<b>Purpose</b>
Splunk	Security monitoring
ServiceNow	Incident tracking
Okta	Identity management
CrowdStrike	Endpoint protection
Veeam	Backup & recovery

---

## **9. Review Cycle**

This SOP is reviewed annually or after major incidents.