STANDARD OPERATING PROCEDURE

Reporting a Security Incident

Prepared by:
Tawana Chealey

Document ID: SOP-SEC-001
Version: 1.0
Effective Date:
Last Updated:

Confidential - Internal Use Only

Table of Contents

Purpose 3

Scope 3

Responsibilities 3

Procedures 3

Step 1: Identify the Incident 3

Step 2: Report the Incident 4

Step 3: Provide Details About the Incident 4

Step 4: Stop Any Further Investigation 4

Step 5: Follow Up 4

Escalation Criteria 4

Other Resources: 4

Document History / Revision Log 5

Purpose

The purpose of this Standard Operating Procedure (SOP) is to provide a clear process for all responsible parties on how to report a security incident that may impact the confidentiality, integrity or availability of organizational systems or data.

Scope

This SOP applies to all employees, contractors, temporary staff and third-party vendors who are able to access Chealey Solutions LLC’s systems, data, or networks.

Responsibilities

Roles	Responsibilities
Employees	Promptly identify and report all suspicious activity
IT Support	Notate and respond to incidents, provide technical guidance and support
Security Team	Investigate, escalate (if applicable) to appropriate leadership, and document the outcomes
Management	Provide awareness and ensure compliance with incident reporting policies

Procedures

Step 1: Identify the Incident

Detect signs of compromised security events, such as:

- Abnormal system behavior
- Unauthorized access alerts
- Phishing emails
- Virus detections

Step 2: Report the Incident

Notify the Security Team immediately via one of the following:

- Email: info@chealeysolutions.com
- Phone: (704) 605-5730
- Incident Form: [link goes here]

Step 3: Provide Details About the Incident

Details that must be included:

- Time/Date of incident was discovered
- Description of incident
- Who or what was affected? (i.e., systems, users)
- Were any other actions taken?

Step 4: Stop Any Further Investigation

Do not delete any files or proceed with our own investigation unless directed by the Security Team.

Step 5: Follow Up

The Security Team will provide any updates, recommendations or request for user assistance regarding containment or mitigation, if needed.

Escalation Criteria

When should incidents be escalated to senior management?
Incidents should be reported to senior management if they involve the following:

- Personal identifiable information (PII) breaches
- Financial systems
- Extended downtown
- Reputational impact

Other Resources:

- [Insert Acceptable Use Policy]
- [Insert Incident Response Plan]
- [Insert Cybersecurity Training Portal

Version 1.0 | Last Updated: May 1, 2024

Document History / Revision Log

Version	Date	Author	Description of Change
1.0		Tawana Chealey	SOP draft created