# Information Technology Security Incident Response Plan (SRIP)

## Table of Contents

# *IT Security Incident Response Plan*

## Purpose

The purpose of this plan is to protect the confidentiality, integrity and availability of Sarasota County Schools ("SCS") data. The proper handling of information technology security incidents (hereinafter referred to as "security incidents"), both electronic and physical, is critical in protecting SCS. These procedures are intended to coexist with all other legally binding documents that guide the conduct of SCS employees. It is not intended to replace in part, or in whole, pertinent Florida or federal laws. Such laws include the Computer Crimes Act, Chapter 815 of the Florida Statutes; the Public Records Law; Chapter 119 of the Florida Statutes; 501.171 of Florida Statutes for security of confidential personal information; or obscenity and child pornography laws. This plan can be found in the Information Technology area of SCS's website:

*The IT Security Incident Response Plan is organized into four stages.*

## Incident Identification, Containment, and Classification (stage one)

A security incident is a real or perceived threat which exploits or attempts to exploit vulnerability. All SCS employees are responsible for identifying and reporting possible security incidents. While some security incidents appear to be easily identified and understood, others require review and analysis to make a determination about the nature and scope of the problem. Many SCS employees will not be able to confirm a security incident, thus any abnormal events should be reported promptly. Examples of events which should be reported are:

- Password alterations not initiated by the user;
- Internet browser pop-ups that cannot be closed;
- Workstation infection from a virus, worm, spyware or other malicious software;
- Missing physical files that contain data classification: Internal, Sensitive, & Restricted;
- Loss or theft of SCS keys and or ID/Proxy Card which allow facilities access;
- Loss or theft of SCS computer hardware; and
- Loss or theft of any mobile computing device.

All SCS employees must report these and other suspicious events immediately to a member of the Security Incidence Response Team, which consists of all school-based IT staff, System Administrators, Manager Network and Telecommunications Services, and Manager School Support Services (hereinafter referred to as "Security Response Team") during normal business hours. All after-hours security incidents must be reported as soon as possible to the employee's supervisor. Loss or theft of SCS real or personal property must be reported to the employee's supervisor. Security incidents will be documented on SCS's IT Security Incident Response Form (Attachment C).

Here are some general guidelines that should be followed during a possible security incident:

- If your password has been compromised, change it immediately and report the security incident;

- If you have reported a security incident, do not continue working on the computer, or in the case of a physical security incident do not continue working in that area;
- Do not close computer applications, or alter the work area (close or move physical documents, etc.) as this may destroy useful information;
- Do not resume using a workstation or a work area until it is declared 'safe' by the Security Response Team; and
- Only discuss the security incident with the Security Response Team. Only the Security Response Team and the employee's Management are allowed to communicate information about a security incident.

When reporting a potential security incident attention to detail is very important. Keep track of the time and what activities were being performed (in detail) when the potential security incident is discovered. By recording these facts, the Security Response Team will have better information by which to respond to the security incident. **All incidents should also be recorded in the SCS technology ticketing system (HELP) regardless of severity**. The important details to include in reporting a security incident are:

- Name, location, telephone number and workstation name if applicable;
- A detailed description of the potential security incident or abnormal event(s);
- The date(s) and time(s) of when the potential security incident or abnormal event occurred; and
- Any other additional information which can be obtained without affecting or making worse the security incident or which could alert a potential or confirmed perpetrator that someone is aware of their actions or presence.

**The Security Response Team will begin the documentation process.**
Security incidents fall within one of three risk categories. In addition, each of these categories will be associated with a security incident classification level. **IT Security Incident Communications** will be based upon the priority assigned to the security incident. A priority will be assigned to each security incident upon examination and review of the event. Loss, theft or unauthorized disclosure of personally identifiable information will follow the communication as described in FL Statute 501.171.

Only communications authorized by the Director of Information Technology and Superintendent's Office may communicate information about a security incident. Communicating information haphazardly about a security incident could further increase the risk to SCS.

## Risk Levels

| Risk | Description | Examples (not limited to) |
|---|---|---|
| **Low** | A security incident which includes **internal** information. Security incidents at this level include loss of physical or electronic data which is of **limited** risk to SCS. | • Loss, theft, or unauthorized disclosure of data that has minimal impact or risk to SCS or its stakeholders;<br>• Vulnerabilities that can be completely mitigated by changes in configurations, policy, procedure, or through technology; and<br>• Loss, theft, or unauthorized disclosure of a SCS portable or removable storage device that contains data classified as **internal** and which is not encrypted. |
| **Medium** | A security incident which **disrupts normal work** (workstation, local area network, work area). Security incidents at this level may include loss, theft, or unauthorized disclosure of **sensitive** information (which does not include personally identifiable information). Security incidents at this level are of **moderate** risk to SCS. | • Loss, theft, or unauthorized disclosure of electronically stored data classified as **sensitive** electronically stored data which is not encrypted (which does not include personally identifiable information);<br>• Loss, theft, or unauthorized disclosure of physical information which contains data classified as **sensitive** (which does not include personally identifiable information); and<br>• Any security incident which allows an intruder access at a level less than privileged, which could lead to further opportunity to obtain greater access whether electronic or physical. |
| **High** | A security incident affecting a **large number of users** which affects **sensitive** information or any security incident which affects **restricted** information. Security incidents at this level are of **extreme** risk to SCS. | • Virus, worm, or other malicious code propagation without user action;<br>• A security incident which allows an intruder to gain privileged access (admin/root) to a system;<br>• A security incident which allows an intruder to gain unauthorized physical access to a secured facility;<br>• The physical or electronic compromise of confidentiality, integrity, availability of data or the integrity or availability of processing resources;<br>• Loss, theft, or unauthorized access and/or dissemination of personally identifiable information whether physical or electronic;<br>• Loss, theft, or unauthorized disclosure of physical information (manual records) classified as **sensitive in which a large number of users are affected**;<br>• Loss, theft, or unauthorized disclosure of electronic data classified as **sensitive** which is not encrypted.<br>• Loss, theft, or unauthorized disclosure of electronic data classified as **restricted.** |

## Classification Levels*

| Level | Description | Examples (not limited to:) |
|---|---|---|
| **Public** | Data can be disclosed without restriction. | Directories, Course Materials, de-identified data sets, etc. |
| **Internal** | Confidentiality of data is preferred, but information contained in data may be subject to open records disclosure. | Email correspondence, budget plans, etc. |
| **Sensitive** | Data confidentiality required by law, policy, or contractual obligation. | Student records and prospective student records (w/o Social Security Numbers), Critical infrastructure information (IT systems info, system passwords, etc.), Student IDs |
| **Restricted** | Restricted data requires privacy and security protections. Special authorization may be required for use and collection. | Data sets with individual SSNs (or last four of SSN), credit card data, financial data, etc. |

## Investigation (stage two)

In the investigation stage, the Security Response Team will gather all known information regarding the security incident and will correlate any information regarding the current incident to any other incidents and abnormal events to determine the urgency and the scope of the issue. Criteria that determine the severity and urgency are:

- Business Criticality
- System Availability
- Data Availability
- Level of current functionality
- Effect on employee productivity
- Lack of alternative workarounds
- Data classification level of information
- Loss, theft, unauthorized disclosure of personally identifiable information

If it is determined that no security incident has occurred, the suspected incident will be labeled as an event and closed by the Security Response Team. If the risk is determined to be low, it will be documented in the SCS technology ticketing system only and closed. No form will be completed.

## Notification/Alerting and Responding (stage three)

In the notification and response stage the Security Response Team will determine the scope of the security incident, the immediate impact, and initiate the required response. Escalation and communication alerts are the responsibility of the Security Response Team. Should the security incident meet any of the following criteria, the escalation process should be immediately followed:

- Security incident has an immediate enterprise wide impact;
- Security incident meets legal requirements that require disclosure; or

- Security incident has caused a business critical service interruption.

Attachment A details the IT Security Incident Response Communications Plan and priorities that the Security Response Team will follow.

### Escalation

In the event that the security incident has immediate impact on SCS as a whole, the Security Response Team investigating the security incident will promptly notify the Director of Information Technology. Certain security incidents may require reporting or alerting of outside third parties or vendors.

## Reporting and Documentation (stage four)

All Medium and High Level security incidents will be documented through the use of the IT Security Incident Response Form. All employees involved in a security incident are required to provide feedback and documentation on their involvement in the process. At a minimum, the report will contain the following information collected during each stage of a security incident investigation:

- Name, location, telephone number and workstation name if applicable;
- A detailed description of the potential security incident or abnormal event(s);
- The date(s) and time(s) of when the potential security incident or abnormal event occurred; and
- Any other additional information which can be obtained without affecting or making worse the security incident or which could alert a potential or confirmed perpetrator that someone is aware of their actions or presence;
- Security Response Team staff member who investigated the security incident;
- Cause of the security incident (if apparent);
- Employee(s) involved;
- Action(s) taken;
- Resolution;
- Date completed;
- Business impact;
- Damage caused;
- Lessons learned;

Planned future mitigation (if possible).

Attachment B provides guidance in developing a detailed security incident response report.

## IT Security Incident Response Communications Plan

**IT Security Incident Communications** will be based upon the priority assigned to the security incident. A priority will be assigned to each security incident upon examination and review of the event. Loss, theft or unauthorized disclosure of personally identifiable information will follow the communication requirements as described by law.

Only communications authorized by the Director of Information Technology and Superintendent's Office may communicate information about a security incident. Communicating information haphazardly about a security incident could further increase the risk to SCS.

The priority of an incident is based on the applicable risk level.

Priority Low security incidents require the Security Response Team to enter a ticket into the SCS technology ticketing system, if not already entered and notify designated persons of the affected areas as required. If ticket is already created, the person will be notified by the system upon commencement of work. In the event that the SCS technology ticketing system is unavailable, the information will be dispersed by telephone or email. The communication will state:

- What non-critical device/system is affected;
- That the incident is being worked on; and
- Estimated time to resolution.

Priority Medium security incidents require the Security Response Team to create an e-mail which will be sent to the employee's management and to other designated persons as required.
In the event that SCS's e-mail system is unavailable, the information will be dispersed by telephone. The communication will state:

- What the security incident is;
- What workstation, device, laptop, etc., has been affected;
- That the incident is being worked on; and
- Estimated time to resolution.

Priority High security incidents require the Security Response Team to create an e-mail for dispersion that will be delivered to all persons affected. In addition, the Security Response Team will notify the main point of contact for all facilities affected by telephone. The communication will state:

- What the security incident is;
- What systems or availability of systems the incident has affected;
- That the incident is being worked on;
- Estimated time to resolution;
- Updates will be forthcoming; and
- State any prescribed course of action the customers must take until the incident is resolved.

# IT Security Incident Response Guidelines

**IT Security Incident Response Reports** are required on all security incidents that the Security Response Team responds to. The following information is provided as a guideline for developing detailed security incident response reports. At the conclusion of each report, there must be a recommended course of action that specifies what should be done to prevent the future reoccurrence of the security incident.

## Preparation

- Were detection capabilities in place that discovered this incident?
- Were security controls in place to prevent the security incident?
- What conditions allowed the security incident to happen?
- What could have prevented this security incident?
- Was this security incident reported promptly?

## Detection

- How soon after this security incident occurred was it detected?
- What could have been done to detect this earlier?
- Was the IT Security Incident Response Policy followed?
- Did the Security Response Team respond in a prompt manner?
- Were the required parties informed of the security incident?

## Containment

- How quickly was the security incident contained?
- What was done to contain the security incident?
- If services were disrupted to SCS to contain this security incident, was the Director notified?
- If services were disrupted to SCS to contain this event, was SCS Security Response Team notified?
- Could changes be made to the environment that would have made containing the security incident easier or faster?
- Were all containment actions documented?
- Was criminal activity involved?
- Was appropriate action taken or sought?
- Criminal intent?
- Was notification completed as required by law or statute?

## Corrective Action

- Was the security incident corrected?
- Was data recovered if involved, and was any data permanently lost or compromised?

- How were corrective actions prioritized if the security incident covered multiple devices, systems, or locations?
- Were the necessary tools readily available to support the corrective actions taken?
- Did the staff have the necessary training to determine and implement the necessary corrective actions to remedy the security incident?

## Incident Review

- What could be done to prevent this security incident from reoccurring?
- What security controls could be put in place to protect or detect against security incidents of this nature?
- What training or education could be implemented to solve or prevent security incidents of this type?
- What was learned from this security incident?

# Security Incident Response Report

| Incident ID: Unique Identifier | Vulnerability: **List the vendor-specific vulnerability number or CVE number, if applicable** | Exploit: **Name of worm, virus, trojan, or type of compromise attempted** | Date: **Date** |
|---|---|---|---|

| | |
|---|---|
| **Executive Summary:** | **Three-to-five sentence summary including the incident scope and severity, as well as the impact on the network and customers.** |
| **Background:** | **Background information on the vulnerability and exploit. Should include:**<br>• **A brief description of the vulnerability**<br>• **Links to 3rd party sites that provide further info (such us vendor or AV sites)**<br>• **Reactive measures to recover from the incident, or**<br>• **Links to 3rd party virus removal utilities**<br>• **Proactive measures that could have prevented the incident**<br>• **Length of time that applicable vendor-supplied patches and/or antivirus DAT files have been available** |
| **Description of Incident:** | **Detailed description of the incident. Should include a chronological listing of actions that were taken by Security Response Team staff and other involved staff starting with the discovery of the incident, the potential effects the incident could have on the production network, and the actual effects of the incident. Should not include corrective action, which will be listed below.** |

| | |
|---|---|
| **Corrective Action:** | **Once the incident has been resolved, actions taken by Security Response Team staff and other involved staff to recover from the incident should be listed here. Should include actions such as running virus removal utilities, running vendor-supplied patches, checking for rootkits, and restoring from backups. If the incident is not yet resolved, should include prescribed actions that need to be taken as directed by Security Response Team staff.** |
| **Current Status of the Incident:** | **Current state of the incident.** |
| **Technical Recommendations:** | **Should include both short-term and long-term recommendations from both Security Response Team staff and other involved staff to prevent this type of incident from occurring in the future.** |
| **Cost:** | **If approximate costs can be forecast from the above technical recommendations, those should be listed here. If Security Response Team staff perform an analysis of the cost of the incident (for example, to justify investigation by law enforcement) then the cost of the incident should be included here.** |
| **Schedule:** | **Follow-up actions such as reactive measures and post-mortem meetings should be listed here, as well as hard times for those actions.** |