



# SARASOTA COUNTY SCHOOLS

## Information Technology Data Loss Prevention Plan (DLPP)

### Table of Contents

1.0 Overview .....	2
2.0 Objective / Purpose .....	2
3.0 Scope .....	2
4.0 Standard .....	2
4.1 Classification .....	2
4.1.1 Classifying Data According to Protection Needs .....	2
4.1.2 Classifying Data According to Availability Needs .....	4
4.2 Protection .....	5
5.0 Enforcement and Implementation .....	12
5.1 Roles and Responsibilities .....	12
5.2 Consequences and Sanctions .....	12
6.0 Exceptions .....	12

# Data Classification and Protection Standard

---

## 1.0 Overview

Data assets are some of the most valuable assets owned by the Sarasota County Schools (SCS). SCS produces, collects, and uses many different types of data in fulfilling its mission. Laws and institutional policy mandate privacy and protection of certain types of data, and the District's need to manage the risks to its reputation and to its constituents requires the protection of other information. Classifying data is the first step in determining the data's need for protection.

## 2.0 Objective / Purpose

This standard is intended to help SCS employees classify data for the purposes of determining its need for protection and determining applicable policies and laws.

## 3.0 Scope

This standard can be used to classify any data that are stored, processed, or transmitted by SCS. The standard applies to all types of data:

- Electronic data,
- Data recorded on paper and
- Information shared orally, visually or by other means.

## 4.0 Standard

### 4.1 Classification

Data can be classified either in terms of its need for protection (e.g. Sensitive Data) or its need for availability (e.g. Critical Data). To classify data in terms of its need for protection, use section 4.1.1 of this standard. To classify data in terms of its availability needs, use section 4.1.2 of this standard.

#### 4.1.1 Classifying Data According to Protection Needs

Match any data that needs to be classified to one of the four categories which best describes its need for confidentiality and its risk profile. The four categories are Public, Internal, Sensitive, and Restricted.

##### 4.1.1.1 Public Data

Data can be disclosed without restriction. Examples - Directories, Course Materials, de-identified data sets, etc.

#### **4.1.1.2 Internal Data**

Confidentiality of data is preferred, but information contained in data may be subject to open records disclosure. Examples - email correspondence, budget plans, etc.

#### **4.1.1.3 Sensitive Data**

Data confidentiality required by law, policy, or contractual obligation.

##### **Characteristics of Sensitive Data**

- Compliance Risk: Protection of data is mandated by law (e.g. FERPA) or required by private contract (e.g. non-disclosure agreements).
- Reputation Risk: Loss of confidentiality or integrity will cause significant damage to SCS's reputation. For example, loss of social security numbers or defacement of the SCS website would likely be a news item that would appear in the media.
- Other Risks: Loss of confidentiality that could cause harm to individuals such as SCS students, personnel, and vendors. Loss of confidentiality or integrity that would cause SCS to incur significant costs in response.
- Treatment in Open Records Requests: Sensitive information is typically redacted from open records disclosures.

##### **Examples of Sensitive Data**

- Student records and prospective student records (w/o Social Security Numbers)
- Alumni records
- Critical infrastructure information (physical plant detail, IT systems information, system passwords, information security plans, etc.)
- Research information related to funding, human subject, etc.
- Information protected by non-disclosure agreements (NDAs) or similar private contracts
- Law enforcement and investigative records
- SCS ID Number (also known as the A Number)

#### **4.1.1.4 Restricted Data**

Restricted data requires privacy and security protections. Special authorization may be required for use and collection. Examples - data sets with individual Social Security Numbers (or last four of SSN), credit card data, health data, financial data, etc.

##### **Characteristics of Restricted Data**

- Compliance Risk: Protection of information is mandated by law (HIPAA).
- Reputation Risk: Loss of confidentiality or integrity will cause significant damage to SCS's reputation.
- Other Risks: Loss of the confidentiality or integrity of the information that could cause harm to individuals and cause the District to incur significant costs in response.
- Treatment in Open Records Requests: Records with restricted information are typically not open for public inspection.

## **Examples of Restricted Data**

- Social Security Numbers (or last four numbers of an individual's SSN)
- Credit/debit card data
- Healthcare data
- Financial account data

## **4.1.2 Classifying Data According to Availability Needs**

Match any data that needs to be classified according to availability needs to one of the three categories which best describes its need for availability needs. The three categories are Supportive, High-Priority, and Critical.

### **4.1.2.1 Supportive Data**

Supportive data is necessary for day-to-day operations, but is not critical to the District's or to a Department's/School's mission or core functions. Examples - course materials, meeting minutes, workstation images, etc.

### **4.1.2.2 High-priority Data**

Availability of data is necessary for departmental function. Destruction or temporary loss of data may have an adverse effect on school or departmental mission, but would not affect District-wide function.

### **4.1.2.3 Critical Data**

Critical data has the highest need for availability. If the information is not available due to system downtime, modification, destruction, etc., the District's functions and mission would be impacted. Availability of this information must be rigorously protected.

#### **Characteristics of Critical Data**

- **Mission Risk:** Short-term or prolonged loss of availability could prevent SCS from accomplishing its core functions or mission.
- **Health and Safety Risk:** Loss of availability may create health or safety risk for individuals. (e.g. emergency notification data, health data, etc.).
- **Compliance Risk:** Availability of information is mandated by law (HIPAA) or required by private contract.
- **Reputation Risk:** Loss of data will cause significant damage to SCS's reputation.

#### **Examples of Critical Data**

- Emergency notification/contact data
- Health care data
- Student records

## 4.2 Protection

See the table below for minimum standard protection requirements for each category of data when being used or handled in a specific context (e.g. Sensitive Data sent in an email message). Please note that the below protection standards are not intended to supersede any regulatory or contractual requirements for handling data. Some specific data sets, such as student records data, credit/debit card data, healthcare data, and financial account data, may have stricter requirements in addition to the minimum standard requirements listed below.

	Public Data	Internal Data	Sensitive Data	Restricted Data
<b>Collection and Use</b>	No protection requirements	No protection requirements	Limited to authorized uses as outlined in the SCS Board Policy 3.50.	<p>Limited to authorized uses as outlined in the SCS Board Policy 3.50.</p> <p>SSNs may not be used to identify members of the SCS community if there is a reasonable alternative.</p> <p>SSNs shall not be used as a username or password.</p> <p>SSNs shall not be collected on unauthenticated individuals.</p> <p>All credit/debit card uses must be approved by the SCS Finance Office.</p>

<p><b>Granting Access or Sharing</b></p>	<p>No protection requirements</p>	<p>Reasonable methods shall be used to ensure internal data is accessed by or shared with authorized individuals or individuals with a legitimate need to know.</p>	<p>Access shall be limited to authorized District officials or agents with a legitimate academic or business interest and a need to know.</p> <p>All access shall be approved by an appropriate data owner and tracked in a manner sufficient to be auditable.</p> <p>Before granting access to external third parties, contractual agreements which outline responsibilities for security of the data shall be approved by the District.</p>	<p>Access shall be limited to authorized District officials or agents with a legitimate academic or business interest and a need to know.</p> <p>All access shall be approved by an appropriate data owner and tracked in a manner sufficient to be auditable.</p> <p>Before granting access to external third parties, contractual agreements which outline responsibilities for security of the data shall be approved by the District.</p>
--	-----------------------------------	---	---	---

<p><b>Disclosure, Public Posting, etc.</b></p>	<p>No protection requirements</p>	<p>Reasonable methods shall be used to ensure internal data is only disclosed to authorized individuals or individuals with a legitimate need to know.</p>	<p>Sensitive data shall not be disclosed without consent.</p> <p>Sensitive data may not be posted publicly.</p> <p>Directory information can be disclosed without consent. However, per FERPA, individual students can opt out of directory information disclosure.</p>	<p>Not permitted unless required by law.</p>
<p><b>Electronic Display</b></p>	<p>No protection requirements</p>	<p>Reasonable methods shall be used to ensure internal data is only displayed to authorized individuals or individuals with a legitimate need to know.</p>	<p>Only to authorized and authenticated users of a system.</p>	<p>Restricted data shall be displayed only to authorized and authenticated users of a system.</p> <p>Identifying numbers or account number shall be, at least partially, masked or redacted.</p>

<p><b>Open Records Requests</b></p>	<p>Data can be readily provided upon request. However, individuals who receive a request must coordinate with the SCS Communications Director.</p>	<p>Individuals who receive a request must coordinate with the SCS Communications Director.</p>	<p>Sensitive data is typically not subject to open records disclosure. However, some open records requests can be fulfilled by redacting sensitive portions of records. Individuals who receive a request must coordinate with the SCS Communications Director.</p>	<p>Restricted data is typically not subject to open records disclosure. However, some open records requests can be fulfilled by redacting sensitive portions of records. Individuals who receive a request must coordinate with the SCS Communications Director.</p>
<p><b>Exchanging with Third Parties, Service Providers, Cloud Services, etc.</b></p>	<p>No protection requirements</p>	<p>Reasonable methods shall be used to ensure that the third party's responsibilities for confidentiality / privacy of the data are defined and documented.</p>	<p>A contractual agreement (or MOU if governmental agency) outlining security responsibilities shall be in place and approved by the District before exchanging data with the third party / service provider.</p>	<p>A contractual agreement (or MOU if governmental agency) outlining security responsibilities shall be in place and approved by District before exchanging data with the third party / service provider.</p>
<p><b>Storing or Processing: Server Environment</b></p>	<p>Servers that connect to the SCS Network shall comply with minimum security standards for networked devices.</p>	<p>Servers that connect to the SCS Network shall comply with minimum security standards for networked devices.</p>	<p>Servers shall comply with security standards for networked devices.</p>	<p>Servers shall comply with security standards for networked devices.  Storing Credit/Debit card PAN data is not permitted.</p>



<p><b>Storing or Processing: Endpoint Environment (e.g. laptop, phone, desktop, tablet, etc.)</b></p>	<p>Systems that connect to the SCS Network shall comply with minimum security standards for networked devices</p>	<p>Systems that connect to the SCS Network shall comply with minimum security standards for networked devices</p>	<p>Systems shall comply with security standards for networked devices</p>	<p>Systems shall comply with security standards for networked devices.</p> <p>Storing Credit/Debit card PAN data is not permitted.</p> <p>Storing restricted data on personally-owned devices is not permitted.</p>
<p><b>Storing on Removable Media (e.g. thumbdrives, CDs, tape, etc.)</b></p>	<p>No protection requirements</p>	<p>No protection requirements</p>	<p>Sensitive data shall only be stored on removable media in an encrypted file format or within an encrypted volume.</p>	<p>Not permitted unless required by law.</p> <p>If required by law, data stored on removable media shall be encrypted and the media shall be stored in a physically secured environment. Storing restricted data on personally-owned media is not permitted.</p>
<p><b>Electronic Transmission</b></p>	<p>No protection requirements</p>	<p>No protection requirements</p>	<p>Data shall be transmitted in either an encrypted file format or over a secure protocol or connection.</p>	<p>Secure, authenticated connections or secure protocols shall be used for transmission of restricted data.</p>

<p><b>Email and other electronic messaging</b></p>	<p>No protection requirements</p>	<p>Reasonable methods shall be used to ensure internal data is only included in messages to authorized individuals or individuals with a legitimate need to know.</p>	<p>Sensitive data shall only be included in messages within an encrypted file attachment.</p> <p>Messages shall only be sent to authorized individuals or other individuals with a legitimate need to know.</p>	<p>Not permitted unless required by law.</p> <p>If required by law, data shall be included in an encrypted file that is attached to the message.</p>
--	-----------------------------------	---	---	--

<p><b>Printing, mailing, fax, etc.</b></p>	<p>No protection requirements</p>	<p>Reasonable methods shall be used to ensure that printed materials are only distributed or available to authorized individuals or individuals with a legitimate need to know.</p>	<p>Printed materials that include sensitive data shall only be distributed or available to authorized individuals or individuals with a legitimate need to know.</p> <p>Access to any area where printed records with sensitive data are stored shall be limited by the use of controls (e.g. locks, doors, monitoring, etc.) sufficient to prevent unauthorized entry.</p>	<p>Printed materials that include restricted data shall only be distributed or available to authorized individuals or individuals with a legitimate need to know.</p> <p>Access to any area where printed records with restricted data are stored shall be limited by the use of controls (e.g. locks, doors, monitoring, etc.) sufficient to prevent unauthorized entry.</p> <p>Social Security Numbers shall not be printed on any card required to access services.</p> <p>New processes requiring the printing of SSN on mailed materials shall not be established unless required by another state agency or a federal agency.</p>
--	-----------------------------------	---	---	---

<b>Disposal</b>	No protection requirements	No protection requirements.	Data shall be deleted and unrecoverable (e.g. eraser, zero-fiil, DoD multipass, etc.).  Physical media (e.g. paper, CD, tape, etc.) should be destroyed so that data on the media cannot be recovered or reconstructed.	Data shall be deleted and unrecoverable (e.g. eraser, zero-fiil, DoD multipass, etc.).  Physical media (e.g. paper, CD, tape, etc.) should be destroyed so that data on the media cannot be recovered or reconstructed.
-----------------	----------------------------	-----------------------------	---	---

**5.0 Enforcement and Implementation**

**5.1 Roles and Responsibilities**

Each District department/unit is responsible for implementing, reviewing and monitoring internal policies, practices, etc. to assure compliance with this standard.

**5.2 Consequences and Sanctions**

Non-compliance with these standards may incur the same types of disciplinary measures and consequences as violations of other District policies, including progressive discipline up to and including termination of employment or, in the cases where students are involved, reporting of a Student Code of Conduct violation.

Any device that does not meet the minimum security requirements outlined in this standard may be removed from the SCS network, disabled, etc. as appropriate until the device can comply with this standard.

**6.0 Exceptions**

Exceptions may be granted in cases where security risks are mitigated by alternative methods, or in cases where security risks are at a low, acceptable level and compliance with minimum security requirements would interfere with legitimate academic or business needs. To request a security exception, contact the SCS Director of Information Technology.