	Technology Services Performance Excellence, Cyber Security, and Customer Care Center	**SOP #** PE-CS01	TS -PE-CS11
		Revision #	
		Implementation Date	02/07/2018
Page #	1 of 2	**Last Reviewed/Update Date**	04/07/2018
SOP Owner	Jennifer Miller	**Approval**	Jennifer Miller
SOP Name	Data Breach Response – Securing the Data		

Standard Operating Procedure

1. Purpose

The purpose of this procedure is to document the process to secure data effectively on district devices.

2. Scope

This procedure is intended for all devices.

3. Definition

A data breach is any instance in which there is an unauthorized release or access of PII or other information not suitable for public release. This definition applies regardless of whether an organization stores and manages its data directly or through a contractor or vendor, such as a cloud service provider. Data breaches can take many forms including:

- hackers gaining access to data through a malicious attack;
- lost, stolen, or temporary misplaced equipment (e.g., laptops, mobile phones, portable thumb drives, etc.);
- employee negligence (e.g., leaving a password list in a publicly accessible location, technical staff misconfiguring a security service or device, etc.); and
- policy and/or system failure (e.g., a policy that doesn't require multiple overlapping security measures – if backup security measures are absent, failure of a single protective system can leave data vulnerable). Absent backup procedures can lead to data loss, but do not make it more likely that data will be stolen or shared.

4. Responsibilities

It is the responsibility of Technology Services to ensure the process is completed

5. Process

A	**Establish and implement a written data breach response policy.**	
1	Incorporate applicable breach notification legal requirements.	Cybersecurity team
2	Address data breach response strategy, goals, and requirements.	Cybersecurity team
3	Specify incident handling procedures, strategies for deciding on the course of action in a given situation, and procedures for communication with organizational leadership and outside parties/law enforcement.	Cybersecurity team
4	Establish employee expectations in conjunction with Human Resources (HR) policy and/or employee agreements.	Cybersecurity team
5	Identify the incident response team.	Cybersecurity team
6	Conduct regular reviews of the policy to include any necessary improvements and ensure that it reflects up-to-date federal, State, and local requirements.	Cybersecurity team
7	Identify a team manager who will be in charge of the incident response (with at least one other person designated to assume authority in the absence of the manger)	James Costello
8	Assign and establish team roles and responsibilities, along with specific access credentials.	Cybersecurity team

	Technology Services Performance Excellence, Cyber Security, and Customer Care Center	**SOP #** PE-CS01	TS -PE-CS11
		Revision #	
		Implementation Date	02/07/2018
Page #	2 of 2	**Last Reviewed/Update Date**	04/07/2018
SOP Owner	Jennifer Miller	**Approval**	Jennifer Miller
SOP Name	Data Breach Response – Securing the Data		

B	**Review information system(s) data and identify where PII and other sensitive information resides, and what security controls protect the data.**	
1	Document what PII and other sensitive information is maintained, where it is stored (include backup storage and archived data), and how it is kept secure.	Cybersecurity team
2	Conduct regular risk assessments and evaluate privacy threats, as well as any contractors, vendors, and other business partners.	Cybersecurity team
3	Review who is approved for access to PII and/or other sensitive information and check user activity status to determine which accounts should be deactivated after a pre-determined period of inactivity.	Cybersecurity team
4	Review separation of duties to help ensure integrity of security checks and balances.	Cybersecurity team
5	Implement mitigation controls designed to prevent and detect unauthorized access, theft, or misuse of PII and/or other sensitive data.	Cybersecurity team, Device Imaging & Integration team
6	Implement security controls, such as encryption of sensitive data in motion and at rest (where feasible).	Cybersecurity
7	Regularly review and keep up-to-date data destruction policies, to minimize the risk of data breaches through unauthorized access to archived media or computers that are no longer in use.	Cybersecurity team
C	**Continuously monitor for PII and other sensitive data leakage and loss.**	
1	Employ automated tools, like Intrusion Detection/Prevention Systems, next generation firewalls, and anti-malware tools to monitor and alert about suspicious or anomalous activity.	Enterprise Communication Networks and Cybersecurity team
2	Use Data Loss Prevention solutions to track the movement and use of information within our system, to detect and prevent the unintentional disclosure of PII and/or other sensitive data, for both data at rest and data in motion.	Enterprise Communication Networks
3	Conduct regular searches of the information system and physical storage areas to identify PII that may be outside of approved areas (e.g., scan your network for policy violations or occasionally police open areas for PII left unattended on desks).	Enterprise Communication Networks and Cybersecurity team
4	Conduct internet searches to locate (and, whenever possible, remove) information that is already in the public domain or visible to the public.	Cybersecurity team
5	Periodically test and check privacy and information security controls (e.g., through the use of “real-life” exercises) to validate their effectiveness as part of a risk management program.	Cybersecurity team
D	**Conduct frequent privacy and security awareness trainings as part of an on-going training and awareness program.**	
1	Provide mandatory privacy and information security training on a recurring basis to all employees, school officials, contractors, and any other staff involved in data-related activities.	Cybersecurity team / KnowBe4 training
2	Post and communicate privacy policies to customers and users (for instance, on the CFISD web page or on a bulletin board at the office, through statements inserted in documents or emails, etc.).	Performance Excellence
3	Clearly define and make easily accessible processes for reporting privacy incidents and complaints (depending on the nature of the event, this may include reporting to the authorities, public, and/or individuals affected).	Performance Excellence