	Technology Services Performance Excellence, Cyber Security, and Customer Care Center	**SOP #** PE-CS01	TS -PE-CS01
		Revision #	3
		Implementation Date	02/07/2018
Page #	1 of 3	**Last Reviewed/Update Date**	03/27/2018
SOP Owner	Jennifer Miller	**Approval**	Jennifer Miller
SOP Name	Data Breach - Responding to the Breach		

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 temporarily 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	**Validate the data breach**	
1	Do not assume that every identified incident is actually a breach of PII.	Customer Care Center and Cybersecurity team
2	Examine the initial information and available logs to confirm that a breach has occurred.	Cybersecurity team
3	If possible, identify the type of information disclosed and estimate the method of disclosure (internal/external disclosure, malicious attack, or accidental).	Cybersecurity team
B	**Once a breach has been validated, immediately assign an incident manager to be responsible for the investigation**	
1	Assign a senior level manager, such as the Chief Information Security Officer or an individual at an equivalent director level position, to serve as an incident manager to coordinate multiple organizational units and the overall incident response. (Typically, the team manager is the incident manager; alternatively, the team manager assigns another individual to lead the response activities.)	Cybersecurity team
2	Begin breach response documentation and report process.	Cybersecurity team
3	Coordinate the flow of information and manage public message about the breach.	Cybersecurity and Performance Excellence teams

C	**Assemble the incident response team**	
1	Include representatives from management, information technology, legal, public affairs/media relations, risk management, finance, and audit departments (and possible HR, for internal incidents) in the incident response team.	Disaster Recovery teams
2	Immediately determine the statues of the breach (active, on-going, or post breach).	Cybersecurity team
3	If the breach is active or on-going, take action to prevent further data loss by securing and blocking unauthorized access to systems/data and preserving evidence for investigation.	Cybersecurity team
4	Document all mitigation efforts for later analysis.	Cybersecurity team
5	Advise staff who are informed of the breach to keep breach details in confidence until notified otherwise.	Leadership team
D	**Determine the scope and composition of the breach**	
1	If criminal activity is suspected, notify law enforcement and follow any applicable federal, State, or local legal requirements related to the notification of law enforcement. (The decision to involve outside entities, including law enforcement, should generally be made in consultation with executive leadership and legal counsel.)	CFISD Police Department
2	Identify all affected data, machines, and devices.	Cybersecurity team
3	Conduct interviews with key personnel and document facts (if criminal activity is suspected, coordinate these interviews with law enforcement).	Cybersecurity team
4	When possible, preserve evidence (backups, images, hardware, etc.) for later forensic examination.	Cybersecurity team
5	Locate, obtain, and preserve (when possible) all written and electronic logs and records applicable to the breach for examination.	Cybersecurity team
E	**Notify the data owners**	
1	Reach out to data owners as soon as possible to notify them about the breach. Provide notification in a straightforward and honest manner; avoid evasive or incomplete notifications.	Performance Excellence
2	Foster a cooperative relationship between the incident response team and data owners.	Performance Excellence
3	Work collaboratively with data owners to secure sensitive data, mitigate the damage that may arise from the breach, and determine the root cause(s) of the breach to devise mitigation strategies and prevent future occurrences.	Cybersecurity team
4	If the breach represents a threat to affected individuals' identity security, consider provide credit monitor or identity theft protection services to mitigate the risk of negative consequences for those affected.	Leadership team
5	Make every attempt to avoid news of the breach reach the media before notification of affected individuals has occurred.	Communications Department
6	Work closely with public affairs or media relations staff to craft the appropriate media notification (mailings, emails, phone calls, etc.).	Communications Department

H	**Collect and review any breach response documentation and analyses reports**	
1	Assess the data breach to determine the probable cause(s) and minimize the risk of future occurrence.	Cybersecurity, ECN, NMO teams
2	Address and/or mitigate the cause(s) of the data breach.	Cybersecurity team
3	Solicit feedback from the responders and any affected entities.	Cybersecurity team
4	Review breach response activities and feedback from involved parties to determine response effectiveness.	Cybersecurity team
5	Make necessary modifications to the exist breach response strategy to improve the response process.	Cybersecurity team
6	Enhance and modify your information security and train programs, which includes develop countermeasures to mitigate and remediate pervious breaches; lessons learned must be integrated so that past breaches do not reoccur.	Cybersecurity team