District Public Employee and Partner Agreement
Data Security and Privacy Policy

District Public ("DP") uses student data only for the purposes of assisting schools in better serving their students. As a DP employee, partner, or contractor ("employee"), you are responsible for taking all reasonable efforts to protect student and company data from unauthorized use. Below are the steps you are required to take in order to do so:

1. Data sharing. Never share any student, school, or company data with anyone besides DP staff or the school principal or staff to whom it pertains, except to those the school principal has provided consent to share it with.

1. Personally identifiable data: Personally identifiable data is any data which includes individuals' names and information. Never request personally identifiable data not needed for analysis. Examples of information that is generally not needed for analysis include home addresses and telephone numbers. When such data is inadvertently acquired by District Public immediately remove it from any and all files in which it appears.

2. Data storage: Only store personally identifiable data on the Google Drive folders that are shared exclusively with DP staff and the school principal and staff to whom the data pertains. District Public will request all data to be sent from principals via a designated "Files Received from School" Google Drive folder set up for each client school and will provide principals instructions on how to post files there.

3. Data removal: Remove any analysis or raw data that includes student data from other locations on which it may temporarily reside, including, but limited to, emails and downloads folders, at least once every two weeks.

4. DP computer and email use: All data analysis by DP employees must be done only on DP-owned devices. While DP contractors may conduct DP work on their own devices, these devices adhere to the same requirements as DP owned devices. All devices on which DP work is conducted must have full hard drive encryption and must have anti-virus software installed and running. All DP business must be conducted exclusively using @district-public.com email addresses. Emails that contain student data must be deleted as soon as the file has been retrieved and saved down into DP's encrypted drive. Devices must be kept secure from theft at all times.

5. Two-factor authentication: Employees are responsible for maintaining two-factor authentication on their @district-public.com email addresses and Google Drive access.

6. Ongoing cyber secuirty awareness training: Employees and partners are required to engage with ongoing cyber security awareness training, which will be assigned by District Public.

Other cyber security policies:

District Public:

- Maintains endpoint encryption on all DP owned devices
- Deploys next generation antivirus protection on all DP owned devices

- Deploys anti-phishing and email filtering on all DP email accounts
- Deploys 24-7 cloud backup
- Deploys two-factor authentication on all DP email accounts and shared drive accounts
- Maintains a cyber insurance policy

District Public Cybersecurity Incident Response Plan

EXECUTIVE SUMMARY

To maintain the trust of our employees, customers, and partners and meet regulatory requirements, it is essential that we do everything we can to protect confidential information and systems in the face of a cyberattack. The better prepared we are to respond to a potential cyberattack, the faster we can eradicate any threat and reduce the impact on our business.

This document describes the plan for responding to information security incidents at District Public. This document will explain how to detect and react to cybersecurity incidents and data breaches, determine their scope and risk, respond appropriately and quickly, and communicate the results and risks to all stakeholders.

Effective incident response involves every part of our organization, including IT teams, legal, technical support, human resources, corporate communications, and business operations. It is important that you read and understand your role as well as the ways you will coordinate with others.

This plan will be updated annually to reflect organizational changes, new technologies and new compliance requirements that inform our cybersecurity strategy. We will conduct regular testing of this plan to ensure everyone is fully trained to participate in effective incident response.

ROLES, RESPONSIBILITIES & CONTACT INFORMATION

This Security Incident Response Plan must be followed by all personnel, including all employees, temporary staff, consultants, contractors, suppliers and third parties operating on behalf of District Public. All personnel are referred to as 'staff' within this plan.

Below are details about the roles and responsibilities of each member of District Public to prevent and respond to a workplace incident. It is not an exhaustive list of duties but designed to give each employee a general understanding of their role and the roles of other employees in incident response and prevention.

Incident Response Team Responsibilities

The Incident Response Lead is responsible for:

- Making sure that the Security Incident Response Plan and associated response and escalation procedures are defined and documented. This is to ensure that the handling of security incidents is timely and effective.
- Making sure that the Security Incident Response Plan is current, reviewed and tested at least once each year.
- Making sure that staff with Security Incident Response Plan responsibilities are properly trained at least once each year.
- Leading the investigation of a suspected breach or reported security incident and initiating the Security Incident Response Plan when needed.
- Reporting to and liaising with external parties, including pertinent business partners, legal representation, law enforcement, etc., as is required.
- Authorizing on-site investigations by appropriate law enforcement or third-party security/forensic personnel, as required during any security incident investigation. This includes authorizing access to/removal of evidence from site.

Security Incident Response Team (SIRT) members are responsible for:

- Making sure that all staff understand how to identify and report a suspected or actual security incident.
- Advising the Incident Response Lead of an incident when they receive a security incident report from staff.
- Investigating and documenting each reported incident.
- Taking action to limit the exposure of sensitive data and to reduce the risks that may be associated with any incident.
- Gathering, reviewing, and analyzing logs and related information from various central and local safeguards, security measures and controls.
- Documenting and maintaining accurate and detailed records of the incident and all activities that were undertaken in response to an incident.
- Assisting law enforcement during the investigation processes. This includes any forensic investigations and prosecutions.
- Initiating follow-up actions to reduce likelihood of recurrence, as appropriate.

- Determining if policies, processes, technologies, security measures or controls need to be updated to avoid a similar incident in the future. They also need to consider whether additional safeguards are required in the environment where the incident occurred.

All staff members are responsible for:

- Making sure they understand how to identify and report a suspected or actual security incident.
- Reporting a suspected or actual security incident to the Incident Response Lead (preferable) or to another member of the Security Incident Response Team (SIRT).
- Reporting any security related issues or concerns to line management, or to a member of the SIRT.
- Complying with the security policies and procedures of District Public.

Roles, Responsibilities and Contact Information

[Below is a list of roles within an organization required to conduct a comprehensive, coordinated incident response. You should customize this list to match the size, structure, and regulatory and industry requirements of your organization. Include contact information for everyone involved in incident response, both internally and externally. You should keep a hard copy of your incident response plan and contact information accessible.]

ROLE	RESPONSIBILITY	CONTACT DETAILS
INFORMATION SECURITY		
CEO/Partner	Strategic lead. Develops technical, operational, and financial risk ranking criteria used to prioritize incident response plan. Authorizes when and how incident details are reported. Main point of contact for executive team and Board of Directors.	Luke Davenport 347-466-1034 luke@district-public.com
Incident Response Team Lead and Team Members	Central team that authorizes and coordinates incident response across multiple teams and functions through all stages of a cyber incident. Maintains incident response plan, documentation, and catalog of incidents. Responsible for identifying, confirming, and evaluating extent of incidents. Conducts random security checks to ensure readiness to respond to a cyberattack.	Luke Davenport 347-466-1034 luke@district-public.com Som Pati 646-265-6694 somak@district-public.com

Identity and Access Team Lead and Team Members	Responsible for privilege management, enterprise password protection and role-based access control. Discovers, audits, and reports on all privilege usage. Conducts random checks to audit privileged accounts, validate whether they are required, and re-authenticate those that are. Monitors privileged account uses and proactively checks for indicators of compromise, such as excessive logins, or other unusual behavior. Informs incident response team of potential attacks that compromise privileged accounts, validates and reports on the extent of attacks. Takes action to prevent the spread of a breach by updating privileges.	Luke Davenport 347-466-1034 luke@district-public.com
IT Operations and Support (internal)	Manages access to systems and applications for internal staff and partners. Centrally manages patches, hardware and software updates, and other system upgrades to prevent and contain a cyberattack.	Stevens Demorcy stevens@metrotp.com 347-874-1988 Luke Davenport 347-466-1034 luke@district-public.com
Technical Partners (ISP, MSP, Hosting, Testing Partners, etc.)	Manages security controls to limit the progression of a cyberattack across third-party systems and organizations.	Stevens Demorcy stevens@metrotp.com 347-874-1988
Third Party External Incident Response Teams	Coordinates with Internal Response Team to manage risks. Professional Incident response teams help ensure a solid Incident Response process is followed. It is highly recommended that the company identify and prepare an External Response Team that can be available in an emergency IR situation and provide any requested information prior to an	NA

	emergency to help them become familiar with your environment.	
COMPLIANCE		
Legal Counsel	Confirms requirements for informing employees, customers, and the public about cyber breaches. Responsible for checking in with local law enforcement. Ensures IT team has legal authority for privilege account monitoring.	Luke Davenport 347-466-1034 luke@district-public.com with support from Sean Mathey, Mathey + Stern 917-667-3567 sean@matheyandstern.com
Audit & Compliance	Communicates with regulatory bodies, following mandated reporting requirements.	Luke Davenport 347-466-1034 luke@district-public.com
Human Resources	Coordinates internal employee communications regarding breaches of personal information and responds to questions from employees.	Luke Davenport 347-466-1034 luke@district-public.com
Regulatory Contacts	Receives information about a breach according to timeline and format mandated by regulatory requirements.	Luke Davenport 347-466-1034 luke@district-public.com
COMMUNICATIONS		
Marketing & Public Relations Lead	Communicates externally with customers, partners, and the media. Coordinates all communications and request for interviews with internal subject matter experts and security team. Maintains draft crisis communications plans and statements which can be customized and distributed quickly in case of a breach.	Luke Davenport 347-466-1034 luke@district-public.com
Web & Social Media Lead	Posts information on the company website, email, and social media channels regarding the breach, including our response and recommendations for users. Sets up monitoring across social media channels to ensure we receive	Luke Davenport 347-466-1034 luke@district-public.com

	feedback or questions sent by customers through social media.	
Technical Support Lead (Internal)	Provides security bulletins and technical guidance to employees in case of a breach, including required software updates, password changes, or other system changes.	Luke Davenport 347-466-1034 luke@district-public.com
Technical Support Lead (External)	Provides security bulletins and technical guidance to external users in case of a breach.	Luke Davenport 347-466-1034 luke@district-public.com

Testing and Updates

Annual testing of the Incident Response Plan using walkthroughs and practical simulations of potential incident scenarios is necessary to ensure the SIRT are aware of their obligations, unless real incidents occur which test the full functionality of the process.

1. The Incident Response Plan will be tested at least once annually.
2. The Incident Response Plan Testing will test District Public's response to potential incident scenarios to identify process gaps and improvement areas.
3. The SIRT will record observations made during the testing, such as steps that were poorly executed or misunderstood by participants and those aspects that need improvement.
4. The Incident Response Lead will ensure the Security Incident Response Plan is updated and distributed to SIRT members.

INCIDENT RESPONSE PROCESS OVERVIEW

Below is the structured 6-step process followed in this document as defined by the SANS Institute in their Incident Handler's Handbook. The six steps outlined are:

1. **Preparation**—review and codify an organizational security policy, perform a risk assessment, identify sensitive assets, define which are critical security incidents the team should focus on, and build a Computer Security Incident Response Team (CSIRT).
2. **Identification**—monitor IT systems and detect deviations from normal operations and see if they represent actual security incidents. When an incident is discovered, collect additional evidence, establish its type and severity, and document everything.
3. **Containment**—perform short-term containment, for example by isolating the network segment that is under attack. Then focus on long-term containment, which involves temporary fixes to allow systems to be used in production, while rebuilding clean systems.
4. **Eradication**—remove malware from all affected systems, identify the root cause of the attack, and take action to prevent similar attacks in the future.
5. **Recovery**—bring affected production systems back online carefully, to prevent additional attacks. Test, verify and monitor affected systems to ensure they are back to normal activity.
6. **Lessons learned**—no later than two weeks from the end of the incident, perform a retrospective of the incident. Prepare complete documentation of the incident, investigate the incident further, understand what was done to contain it and whether anything in the incident response process could be improved.

Incident Response Checklist

[Below is a reporting template to use for documenting the steps and documentation gathered during your review and response to a cyber incident involving privileged accounts. Make updates to reflect your approved process and the tools you use. Add a responsible party for each step now, so everyone knows what data they need to gather and steps to take when an incident happens.]

To demonstrate and improve the effectiveness of District Public incident response team and security tools, District Public requires a record of all actions taken during each phase of an incident. Supporting documentation is required, including all forensic evidence collected such as activity logs, memory dumps, audits, network traffic, and disk images.

PHASE OF CYBER INCIDENT	ACTION	TEAM MEMBER/ SYSTEM	DAY/TIME ACTION TAKEN
Incident Discovery and Confirmation	Describe how the team first learned of the attack (security researcher, partner, employee, customer, auditor, internal security alert, etc.).	Luke	
	Analyze audit logs and security applications to identify unusual or suspicious account behavior or activities that indicate a likely attack and confirm attack has occurred.	Luke	
	Describe potential attacker, including known or expected capabilities, behaviors, and motivations.	Luke	
	Identify access point and source of attack (endpoint, application, malware downloaded, etc.) and responsible party.	Luke	
	Prepare an incident timeline to keep an ongoing record of when the attack occurred and subsequent milestones in analysis and response.	Luke	
	Check applications for signatures, IP address ranges, files hashes, processes, executables names, URLs, and domain names of known malicious websites.	Luke	
	Evaluate extent of damage upon discovery and risk to systems and privileged accounts. Audit which privileged accounts have been used recently, whether any passwords have been changed, and what applications have been executed. (See Appendix A for more information on Threat Classification).	Luke	
	Review your information assets list to identify which assets have been potentially compromised. Note integrity of assets and evidence gathered. (See Appendix A for more information on Threat Classification).	Luke	
	Diagram the path of the incident/attack to provide an "at-a-glance" view from the	Luke	

	initial breach to escalation and movement tracked across the network.		
	Collect meeting notes in a central repository to use in preparing communications with stakeholders.	Luke	
	Inform employees regarding discovery.	Luke	
	Analyze incident Indicators of Compromise (IOCs) with threat intelligence tools.	Luke	
	Potentially share information externally about breach discovery. You may choose to hold communications during this phase until you have contained the breach to increase your chances of catching the attacker. If so, make sure this aligns with your compliance requirements.	Luke	
Containment and Continuity	Enable temporary privileged accounts to be used by the technical and security team to quickly access and monitor systems.	Luke	
	Protect evidence. Back up any compromised systems as soon as possible, prior to performing any actions that could affect data integrity on the original media.	Luke	
	Force multi-factor authentication or peer review to ensure privileges are being used appropriately.	Luke	
	Change passwords for all users, service, application, and network accounts.	Luke	
	Increase the sensitivity of application security controls (allowing, denying, and restricting) to prevent malicious malware from being distributed by the attacker.	Luke	
	Remove systems from production or take systems offline if needed.	Luke	
	Inform employees regarding breach containment.	Luke	
	Analyze, record, and confirm any instances of potential data exfiltration occurrences across the network.	Luke	
	Potentially share information externally regarding breach containment (website updates, emails, social media posts, tech support bulletins, etc.).	Luke	
Eradication	Close firewall ports and network connections.	Luke	

	Test devices and applications to be sure any malicious code is removed.	Luke	
	Compare data before and after the incident to ensure systems are reset properly.	Luke	
	Inform employees regarding eradication.	Luke	
	Potentially share information externally regarding eradication (website updates, emails, social media posts, tech support bulletins, etc.).	Luke	
Recovery	Download and apply security patches.	Luke	
	Close network access and reset passwords.	Luke	
	Conduct vulnerability analysis.	Luke	
	Return any systems that were taken offline to production.	Luke	
	Inform employees regarding recovery.	Luke	
	Share information externally regarding recovery (website updates, emails, social media posts, tech support bulletins, etc.).	Luke	
Lessons Learned	Review forensic evidence collected.	Luke	
	Assess incident cost.	Som	
	Write an Executive Summary of the incident.	Luke	
	Report to executive team and auditors if necessary.	Luke	
	Implement additional training for everyone involved in incident response and all employees.	Luke	
	Update incident response plan.	Luke	
	Inform employees regarding lessons learned, additional training, etc.	Luke	
	Potentially share information externally (website updates, emails, social media posts, tech support bulletins, etc.).	Luke	

Responsibilities At-a-Glance

Activity	**Role**					

	CSIRT Incident Lead	**IT Contact**	**Legal Representative**	**Communications Officer**	**Management**
Initial Assessment	Owner	Advises	None	None	None
Initial Response	Owner	Implements	Updates	Updates	Updates
Collects Forensic Evidence	Implements	Advises	Owner	None	None
Implements Temporary Fix	Owner	Implements	Updates	Updates	Advises
Sends Communication	Advises	Advises	Advises	Implements	Owner
Check with Local Law Enforcement	Updates	Updates	Implements	Updates	Owner
Implements Permanent Fix	Owner	Implements	Updates	Updates	Updates
Determines Financial Impact on Business	Updates	Updates	Advises	Updates	Owner

Document Control

Document Name:	Security Incident Response Plan
Current Version:	DistrictPublic_IR_Plan_20210709
Plan Owner:	Luke Davenport
Plan Approver:	Som Pati
Date of Last Review:	

APPENDIX A

THREAT CLASSIFICATION

The CIA Triad (Confidentiality, Integrity, and Availability) is a framework for incident classification that helps to prioritize the level of incident response required for a cyberattack.

1. **Confidentiality** – Incidents involving unauthorized access to systems, including privileged account compromise. The more confidential the data or the more important the systems are to the business, the higher the potential impact.
2. **Integrity** – Incidents involving data poisoning, including leveraging a privileged account to corrupt or modify data. The more sensitive the data, the higher the potential impact.
3. **Availability** – Incidents that impact the availability or proper functioning of services, such as Distributed Denial of Service (DDoS) or ransomware, including use of privileged accounts to make unauthorized changes. The more critical the services to the business, the higher the potential impact.

When ranking the level of risk to the organization and the type of incident response required, you must consider the extent to which privileged accounts are compromised, including those associated with business users, network administrators, and service or application accounts. When privileged accounts are involved in the breach, the level of risk increases exponentially as does the response required.

Employee Acknowledgement

By signing below, I agree that I have read and understood District Public’s data security and privacy policy and its incident response plan and that I will make my best effort to follow these policies.

Printed Name: ________________________________

Position: _____________________________________

Signature: ___________________________________ *Date:* _____________