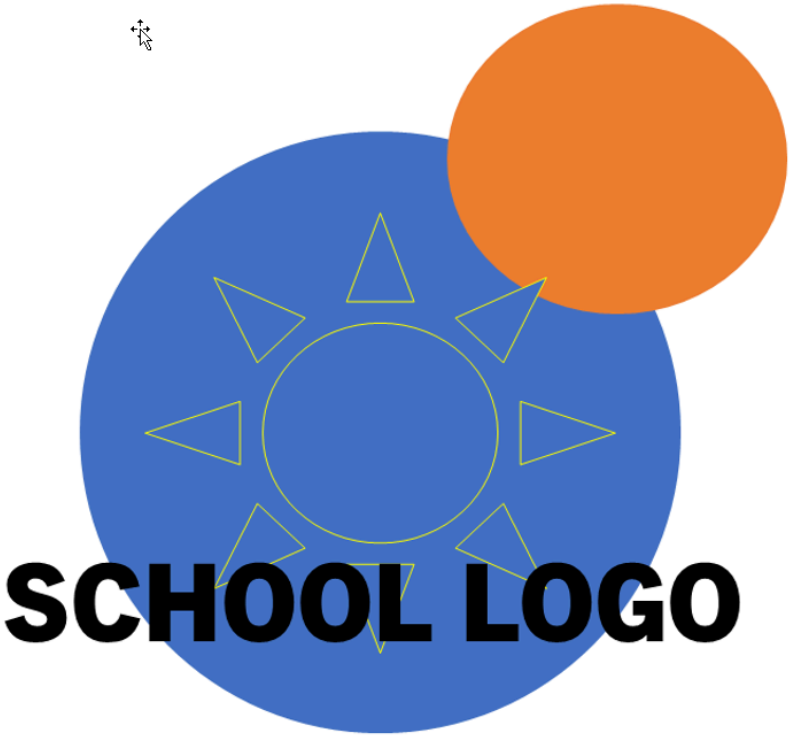

TABLE OF CONTENTS

DOCUMENT REVISION/HISTORY

REVISION	DESCRIPTION OF UPDATE	REVISION DATE	REVISION AUTHOR
0.0	Initial (first) Draft		

1.0 INTRODUCTION

The ***SCHOOL DISTRICT*** Incident Response Plan has been developed to provide direction, information, and focus to the handling of information security incidents. The scope of this plan applies to the physical location (networking closets and data centers), the information systems, all student; personnel; and privileged organization data, and any person or device that gains access to these systems or data.

1.1 DEFINITIONS

- **EVENT** - An exception to the normal operation of infrastructure, systems, or services.
- **INCIDENT**- An event that, as assessed, violates the policies of ***SCHOOL DISTRICT*** as related to information security, acceptable use, code of conduct, or threatens the confidentiality, integrity, or availability of information systems.

1.3 CONTACT INFORMATION

NAME	TITLE	ROLE	CONTACT INFORMATION	ESCALATION*
First Name Last Name	Executive Director of IT Services	**IRMAN** IREST IREVT		1
		IRMAN2 IREST IREVT		3
		IREST IREVT		2
		IREST IREVT		2
		IREST IREVT		2
		IREST IREVT		2
		IREST IREVT		2
		IREST IREVT		2
		IREST IREVT		2
		IREVT		3
		IREVT		2
		IREVT		4
		IREVT		4
NCLGISA Strike Team	North Carolina 3rd Party	IREST IREVT	itstriketeam@nclgisa.org (919) 726-6508	3, 4

***ESCALATION LEVELS**

1. **Notify first**, required for all level incidents.
2. Required for all level incidents.
3. Required for level 2 or level 3 severity incidents.

4. Involve as needed.

1.4.1 ROLES AND RESPONSIBILITIES

1.4.1.1 INCIDENT RESPONSE MANAGER (IRMAN)

The Incident Response Manager oversees all phases of the incident response. Detection, analysis, and containment. This position will be the point for delegating priorities, actions, and communications during and after the incident.

Other responsibilities:

- Report the incident to and engage the North Carolina Local Government Strike Team.
- Review Incident Response Plan and keep all incident response documentation up to date (annually).
- Coordinate tasks and communication to auxiliary departments.
- Manage and coordinate Incident Response Team activities.
- Manage and coordinate Incident Handling Team activities.
- Coordinate and provide incident updates to key stakeholders as requested or as needed.
- Ensure incident documentation is properly logged and filed.
- Plan, coordinate, and execute tabletop exercises with response and handling teams (annually).
- Approve closure of all levels of security incidents.

1.4.1.2 INCIDENT RESPONSE MANAGER II (IRMAN2)

The Incident Response Manager II acts as a backup (secondary) manager to provide the same duties as the IRMAN in the event the IRMAN position/role is vacant or unavailable to perform duties.

1.4.1.3 INCIDENT RESPONSE TEAM (IREST)

The Incident Response Team is comprised of key IT staff including Network Engineers and System Administrators that manage the day-to-day ***SCHOOL DISTRICT*** data, server, and network infrastructure. The team is responsible for promptly containing the incident, investigation, and recovery. The Incident Response Team will work with the NCLGISA Strike Team (see below) as needed for investigation and analysis.

Other Responsibilities:

- Assists in incident response as requested or needed. IREST responsibilities should take priority over normal job duties.
- Understand and follow ***SCHOOL DISTRICT*** incident response plan and procedures.
- Monitor server, system, and network logs for suspicious and unusual activities.
- Participate in tabletop exercises for practice and plan review (annually).
- Coordinate analysis and recovery efforts with NCLGISA Strike Team.

1.4.1.4 INCIDENT RECOVERY TEAM (IREVT)

The Incident Recovery Team is comprised of key ***SCHOOL DISTRICT*** staff including Legal and Communications. This team may be consulted with and needed for providing communications and guidance during the recovery. This team will also help determine the need for additional (3rd party) resources and cyber liability insurance reporting.

Other Responsibilities:

- Advise on incident response activities relevant to their area of expertise.
- Coordinate and report level 2 or 3 level incidents to Cyber Liability Insurance carrier.

- Engage with breach counsel (if needed or recommended by insurance carrier).
- Coordinate and deliver stakeholder communications pertaining to the incident.

1.4.1.5 NCLGISA STRIKE TEAM

The North Carolina Local Government Information Systems Association (NCLGISA) IT Strike Team is comprised of IT management and systems level IT staff from K12 education, local city and county, and state agencies across North Carolina. Additional participating agencies are MCNC (ISP), Friday Institute, and the North Carolina National Guard Cyber Security Response Force (CSRF). The Strike Team members volunteer their time and talents to provide IT support where needed in times of disaster but is also available to any NCLGISA member who needs more resources to address emergency issues.

This team is available 24/7 as an extension of the local incident response team and will assist with incident detection, analysis, containment, and recovery.

1.5 INCIDENT CATEGORIES AND EXAMPLES

Incidents are categorized according to their potential for the exposure of protected data or the criticality of the system.

SEVERITY LEVEL	DESCRIPTION
1 (LOW)	No impact or impact is minimal.
2 (MEDIUM)	Impact is significant. Examples may be a disruption in ***SCHOOL DISTRICT*** provided services. A virus or worm has become widespread and is affecting 1% or more of employees or students. Personnel or student information has been compromised but NOT published on a public venue or site.
3 (HIGH)	Impact is catastrophic. Examples include complete shutdown of ***SCHOOL DISTRICT*** network services, or personnel or student information has been compromised and published on a public venue or site.

EVENT/INCIDENT EXAMPLES:

- Phishing (Account Compromise)
- Malware/Trojans/Keyloggers
- Ransomware attack
- Unauthorized electronic access
- Breach of infrastructure or information (data)

- Unusual, unexplained, and repeated loss of connectivity.
- Company device theft or loss
- Unsecured credentials
- Network denial of service (DDOS) attacks

2.0 INCIDENT RESPONSE FRAMEWORK

2.1 PREVENTION

SCHOOL DISTRICT has implemented multiple layers of system and end user level protections through several initiatives (see table below). These initiatives are designed to help prohibit unauthorized access, or service or data loss.

INITIATIVE	DESCRIPTION
SANITIZE NETWORK AND INTERNET TRAFFIC	
Next Generation Firewalls	Leveraging features such as intrusion prevention, AV scanning, web application filtering and content filtering.
Email Filtering	Filter inbound and outbound emails to reduce phishing and malware attempts made through email. Sandbox scanning provides attachment protection.
Email Protection	Students are not allowed to send mail outside of our domain(s).
Network Segmentation and Fencing	We provide internal site-to-site port blocking and geo fencing restricting logins and some access from US locations only.
Content Filtering	Deep SSL decryption, DNS protection, and content filtering.
SECURE AND SAFEGUARD END USER DEVICES	
Endpoint Protection	Endpoint (EDR) security for all issued ***SCHOOL DISTRICT*** devices has been installed.
ACCOUNT AND IDENTITY PROTECTION	
Multifactor Authentication	MFA has been applied to email, VPN, and all privileged account and server remote access.
Security Awareness Training	Training is provided to all ***SCHOOL DISTRICT*** employees annually.
Privileged Account Access	Privileged access (domain admin, server admin, etc.) has been restricted to separate non-external exposure accounts and workstations.

PERFORM REGULAR MAINTENANCE	
Updates and Patching	Endpoint and Server Patching.
System Logging	Extensive firewall, server, access, and system logging is turned on across all systems and services.
Vulnerability Scanning	Internal and external vulnerability scans are performed both by IT staff and our ISP (MCNC).
Protected Backups	Provide data resilience with immutable data backups.

2.2 PREPARATION

Aside from implementing prevention measures, ***SCHOOL DISTRICT*** will prepare for information security incidents by:

- Establishing, training, and maintaining a cyber security response team.
- Meet monthly with the incident response and incident recovery teams. Ensure each team stays updated and aware of the ***SCHOOL DISTRICT*** incident response plan and reporting processes.
- Improve and maintain documentation, checklists, references, and policies.
- Review vulnerability assessments and validate remediations to findings.
- Perform low, medium, and high-level incident tabletop exercises to ensure processes and procedures and relevant and efficient.

2.3 DETECTION AND ANALYSIS

2.3.1 DETECTION

Detection is the discovery of an event whether it be through user reporting or by a system alert or notification. The Incident Response Manager must perform an initial verification and investigation of an information security event.

There is no single symptom to conclusively prove that a security incident has occurred. The list below contains some symptoms that can be detected:

- Observation of suspicious or anomalous login activity on a system or systems.
- Unexplained attempts to clear system logs.
- Poor system performance of dedicated servers.
- Unusual usage or login patterns.
- Denial/disruption of service or inability of one or more users to login into an account.
- System alerts as to suspicious logins or logins from impossible travel activity.
- System alerts as to the presence of malicious code or malware agents.

2.3.2 ANALYSIS

The incident analysis will be performed in a manner consistent with the type of incident. The incident will be placed into a category based on the severity. Tasks during this phase include:

SCHOOL DISTRICT will develop an incident scope with the following factors:

- What was the entry point for the incident (network, server, user account)?
- How many user accounts are affected?
- How many servers, systems, or services are affected?
- Was data (files folder level, database) accessed or affected?
    - Was the data confidential (personnel or student) or privileged?
- Estimated recovery time to restore or recover systems?

- Export all log files from firewalls, servers and systems for analysis and review.

The Incident Recovery Team will be briefed and updated. The IREVT team will develop their own incident scope with the following factors:

- Was the incident criminal in nature, further action with law enforcement agencies needed?
  - Coordinate with law enforcement if needed.
- Does insurance need to be notified?
  - Determine whether breach counsel needs to be involved.
- Determine need for communication to staff, families, community?

2.3.3 INCIDENT REPORTING

NOTE: Per North Carolina General Statute 143B-1379, SCHOOL DISTRICT must report the incident within 24 hours of verification. The Incident Response Manager will report the incident to the NCLGISA IT Strike Team (see Contact Information) and subsequently engage them in assisting with further analysis and containment.

2.3.3 CONTAINMENT

SCHOOL DISTRICT will contain and lock down the incident based on the level of severity and the number of systems affected. The goal is to regain control and limit the amount of damage (i.e., the immediate shutdown of any threat actor or the prevention of further spread of malicious code). These actions include but are not limited to:

- Immediate removal from network (or shutdown) of affected systems or servers.
- Initiate a system or service wide disconnect or logout of all affected users.
- The installation or implementation of detection or security tools.
- Disable accounts and/or reset passwords.
- Increase activity (and system) logging on affected systems or servers.
- Perform further or more enhanced infrastructure vulnerability assessments.
- Create/capture image scans of servers or workstations affected or compromised (suspected) during or as a result of the incident.

2.3.4 RECOVERY

The recovery phase works to reestablish systems back to normal operation. Depending on the level and severity of the incident, the ***SCHOOL DISTRICT*** Incident Response Team may need to validate the affected systems before putting them back into service. This includes (but not limited to):

- Applying critical security and vulnerability patches.
- Applying updates to code (web page or form) or script to prevent unauthorized access.
- Enabling additional port restrictions in the hardware/software firewalls.
- Disabling or eliminating privileged access accounts from the system.
- Restoring corrupt, missing, or encrypted data from a clean backup prior to the incident.
- Applying deep SSL decryption and web application filter policies at the firewall level.
- Requesting additional external level vulnerability scans.

The ***SCHOOL DISTRICT*** Incident Recovery Team will be involved and provide guidance on the following:

- Continued collaboration or updates with law enforcement agencies.
- Continued collaboration or guidance from breach counsel or outside agency providing incident analysis, response, or recovery services.
- Communications and notifications to staff, students, families, or the community.

2.3.5 POST-INCIDENT

A follow up to the incident recovery process will include reflection and analysis of actions taken during the incident. This process will produce the finalization and closure of the incident report and log (Appendix B).

During this process the Incident Response Plan may need re-evaluated and updated based on reaction and additional needs found during the incident. Considerations taken in account for this include:

- How did staff perform during the incident?
  - Are there corrections needed with roles and duties?
  - Is there additional training needed for the IREST and IREVT teams?
- Can information sharing between organizations or teams be improved?
- Are there additional precursors or indicators that should be watched for in the future?
- Are there additional tools or resources needed to detect, capture, and alert for future incidents?

The content provided in the following (appendix) sections is privileged and confidential information protected by *SCHOOL DISTRICT* specified access.

APPENDIX A (INCIDENT RESPONSE CHECKLIST)

LINK TO SECURE LOCATION

APPENDIX B (INCIDENT LOG AND RECORD TEMPLATE)

LINK TO SECURE LOCATION

APPENDIX D (INCIDENT EXAMPLES AND REMEDIATION STRATEGIES)

LINK TO SECURE LOCATION

APPENDIX E (TABLETOP EXERCISE DOCUMENTATION AND LOG)

LINK TO SECURE LOCATION