CONFIDENTIAL

Client Company

Incident Response Plan

Generated 2026-08-31
Built with FrameworkMapper

FrameworkMapper by Viosoph

Generated from this organization's own security profile, assessment data and recorded contacts. Guidance is drawn from public standards listed in the sources appendix. This document is decision support, not legal advice — confirm reporting obligations with counsel.

Keep a printed or offline copy with your response materials.
A plan reachable only on the network you have just lost is not a plan.

Contents

1. Overview and Purpose

> What this plan is for, who it binds, and what a reader should do with it. State plainly that the plan is authoritative during an incident and that deviations are allowed when they are documented. Approved by senior leadership — name the approving body and the date.

This plan establishes the authority, structure and procedures Client Company uses to respond to cybersecurity incidents affecting district systems, student and staff data, and instructional continuity. It is approved by the Superintendent and is authoritative during an incident; documented deviations are permitted where circumstances require them.

Guidance drawn from: CISA IRP Basics; NIST SP 800-61r3; ISP template

2. Scope and Application

> Which systems, data, sites, business units and third-party services this plan covers, and what it explicitly does not cover. An incident that falls outside the scope still needs an owner, so name where it goes instead.

Applies to all district-owned systems, networks, cloud services and data, at every building, including the student information system, the learning management system, food service, transportation and building automation. Personal devices are in scope only when connected to district systems or holding district data.

Guidance drawn from: NIST SP 800-61r3; ISP template

3. First Hour: Immediate Actions

> The fast path, deliberately placed before the explanatory material so nobody reads an essay at 2am. Six to ten numbered steps: who to call first, how to declare, what to preserve before touching anything, what NOT to do (do not power off, do not alert the adversary, do not discuss on possibly-compromised channels). Everything else in this plan supports this page.

1. Report it: call the Technology Director. If unreachable within 15 minutes, call the Network Administrator.
2. Do not power anything off. Disconnect from the network instead.
3. Do not discuss the incident on district email or Teams until told they are trusted.
4. Write down what you saw and when, with timestamps.
5. The Technology Director declares the incident and notifies the Superintendent.
6. Call the Educational Service Unit for technical support.
7. Preserve: leave affected machines powered on and isolated.

Guidance drawn from: CISA IRP Basics; SANS; CISA Playbooks

4. Plan Distribution and Offline Copies

> During an incident your email, chat and document storage may be down, encrypted, or untrusted. State who holds a printed copy, where offline copies live, and how the contact roster reaches people out-of-band. A plan reachable only from the network it protects is not a plan.

A printed copy of this plan and the contact directory is held in the Technology Director’s office, the Superintendent’s office, and the district office safe. It is reprinted after every review. Assume email, Teams and the file server are unavailable.

Guidance drawn from: CISA IRP Basics

COMMAND AND ROLES

5. Incident Command Roles

> Name the three roles that run the response. Incident Manager: leads, manages communication flow, delegates, watches the clock — and performs NO technical work, because under stress the person doing forensics cannot also run the incident. Technical Manager: the subject-matter lead who pulls in other experts. Communications Manager: handles staff, customers, press and external stakeholders. One person may hold two hats in a small organisation; say which combinations are acceptable.

Incident Manager: Director of Technology. Runs the response, manages communications flow, and performs no technical work during an incident. Technical Manager: Network Administrator. Communications Manager: Communications Director. In a small district one person may hold Incident Manager and Communications Manager, but never Incident Manager and Technical Manager.

Guidance drawn from: CISA IRP Basics; Zscaler

6. Roles and Responsibilities

> Everyone else with a part to play, and what each is accountable for: IT and security staff, asset and data owners, HR, legal, physical security and facilities, executive leadership. NIST is explicit that asset owners hold recovery priorities the response team does not, and that HR and physical security are participants rather than bystanders.

Technology staff perform containment and recovery. The Business Manager owns insurance and vendor contracts. The Communications Director owns all external statements. Building principals are responsible for relaying instructions to staff. District legal counsel is engaged for any incident involving student records.

Guidance drawn from: NIST SP 800-61r3; Zscaler; ISP template

7. Incident Response Team Roster

> The people, with primary and alternate contact methods that do not depend on corporate systems. Include after-hours reachability and at least one contact per role who is not the same person. This is the page most often out of date — say who reviews it and how often.

[To be completed by Client Company]

Guidance drawn from: SANS; CISA IRP Basics; ISP template

8. Incident Detection and Coordination Group

> Who watches for incidents day to day, how a report reaches them, and how they hand off to the response team. Include the monitoring coverage window — an organisation with no overnight coverage should say so here rather than discover it during an incident.

[To be completed by Client Company]

Guidance drawn from: ISP template; NIST SP 800-61r3

9. Incident Risk Management Team

> The group that weighs business risk during a response: whether to take a system offline, whether to pay, whether to notify early. Distinct from the technical team, and named in advance because assembling it mid-incident costs hours.

[To be completed by Client Company]

Guidance drawn from: ISP template; NIST SP 800-61r3

10. Decision Authority and Delegation

> Who can authorise disruptive actions — disconnecting a site, shutting a service, rebuilding a system, engaging outside counsel or spending money. NIST calls out that leadership may hold decision authority on high-impact actions; name the deputy for each so a single absence cannot stall the response.

[To be completed by Client Company]

Guidance drawn from: NIST SP 800-61r3; ISP template

11. Authority to Declare an Incident

> Exactly who may declare, and how they do it out of hours. Under-declaring is the more common failure: make the threshold low and the cost of declaring small.

The Director of Technology may declare an incident at any hour. If unreachable within 30 minutes, the Network Administrator may declare. Declaring is deliberately low-cost: an incident that turns out to be nothing is closed in an hour, and under-declaring has cost districts far more than over-declaring.

Guidance drawn from: CISA Playbooks; ISP template

12. Escalation Paths

> When and to whom a response escalates, with the trigger for each level rather than a judgement call. Include the escalation to executive leadership and to the board.

[To be completed by Client Company]

Guidance drawn from: ISP template; Zscaler

CLASSIFYING AN INCIDENT

13. Incident Declaration

> What turns an event into a declared incident, and what changes the moment it is declared: who is notified, what clocks start, what authorities activate. NIST distinguishes event, adverse event and incident — define all three in your own terms here.

[To be completed by Client Company]

Guidance drawn from: NIST SP 800-61r3; CISA Playbooks

14. Event Categorization

> The incident types you actually see, each with its first-response owner: phishing and account compromise, ransomware, data exfiltration, insider misuse, third-party or supplier compromise, denial of service, lost or stolen device, physical intrusion with a technical element.

[To be completed by Client Company]

Guidance drawn from: CISA Playbooks; ISP template

15. Prioritization

> How competing incidents are ranked. NIST is explicit that prioritization should be based on organisational impact rather than on the order incidents arrive. A workstation offline is minor; a server outage with failover is moderate; data leaving the environment is high.

[To be completed by Client Company]

Guidance drawn from: NIST SP 800-61r3; SANS

16. Severity Levels

> A small, defined ladder — three to five levels — each with observable criteria, a named owner, a notification set and a response time. Severity drives who wakes up; keep it objective enough that two people classify the same incident the same way.

Level 1 — single user or device affected, no data exposure suspected. Technology staff, next business day.
Level 2 — a system or building affected, or exposure suspected. Incident Manager, within 2 hours, Superintendent notified.
Level 3 — district-wide, instruction affected, or confirmed exposure of student or staff data. Superintendent, counsel and carrier engaged immediately, Board notified.

Guidance drawn from: NCIRP; Zscaler; ISP template

17. Functional Impact

> How you describe damage to operations in business terms: which services are degraded or unavailable, for whom, and for how long. This is the language leadership and regulators understand.

[To be completed by Client Company]

Guidance drawn from: NIST SP 800-61r3; ISP template

18. Data Classification and Information Impact

> The data types you hold and what their exposure triggers. This section is what connects the incident to the reporting clocks in the Notification Obligations appendix — PII, PHI, student records, CUI/FCI, payment and financial data each start a different one.

The district holds student education records, staff HR and payroll records, PII for students and families, and limited health information through the school nurse. No CUI or FCI is held. Student records and PII are the exposures that start a notification clock; see the Notification Obligations appendix.

Guidance drawn from: NIST SP 800-61r3; ISP template

19. Incident Reporting Process

> How anyone in the organisation reports something suspicious, in one sentence they can remember. CISA is emphatic on the culture point: be gracious about false alarms and reward people who come forward, or reporting stops.

[To be completed by Client Company]

Guidance drawn from: CISA IRP Basics; ISP template

20. Preparation

> What must be true before an incident to make the rest of this plan executable: logging and retention, backups and tested restores, asset inventory, access to tooling, retainers in place, contacts current. NIST maps this to the Govern, Identify and Protect Functions — preparation is most of incident response.

Maintained in advance: this plan and its printed copy, the contact directory, the ESU support agreement, cyber insurance policy and claims number, quarterly restore tests, and annual staff phishing training.

Guidance drawn from: NIST SP 800-61r3; CISA Playbooks; SANS

21. Establishing Baseline Behavior

> What normal looks like here, recorded before you need it: typical accounts, processes, listening ports, egress destinations, admin activity, logon hours. CISA puts this in Preparation for a reason — deviation is only visible against a baseline.

[To be completed by Client Company]

Guidance drawn from: CISA Playbooks; SANS

22. Detection and Analysis

> Where signals come from and how they are qualified. Distinguish an alert from an adverse event from an incident, and say what evidence is needed to move between them. Note the sources you trust and their retention windows — retention shorter than your detection time is a finding, not a detail.

[To be completed by Client Company]

Guidance drawn from: NIST SP 800-61r3; CISA Playbooks; SANS

23. Triage and Initial Analysis

> The first structured pass: confirm it is real, classify it, size it, assign it. Include the questions that must be answered before containment decisions are made.

[To be completed by Client Company]

Guidance drawn from: SANS; CISA Playbooks

24. Determining Investigation Scope

> CISA calls scoping the hardest part of incident response, and it is iterative: findings feed detection, which finds more. Record what is in scope, what has been ruled out and on what evidence, and revisit both as the picture changes. Prefer adversary behaviours (TTPs) over atomic indicators — infrastructure changes, behaviour is costlier to change.

[To be completed by Client Company]

Guidance drawn from: CISA Playbooks; NIST SP 800-61r3

25. Evidence Preservation and Chain of Custody

> What to capture before it is destroyed by remediation, in what order, and how it is stored and handed over. Forensic images before rebuilds; volatile data before shutdown. Record who held what and when — if the incident becomes a legal matter, chain of custody is the difference between evidence and an anecdote.

Preserve before remediating. Affected machines stay powered on and disconnected. The Network Administrator records who held what and when. Nothing is rebuilt until the Incident Manager confirms evidence has been captured or has explicitly accepted the loss.

Guidance drawn from: SANS; CISA Playbooks

26. Response Operational Security

> Assume the adversary can read your email, your chat and your ticketing system until proven otherwise. State which out-of-band channel the response uses, who is admitted to it, and the rule about not tipping off the adversary before containment is ready. CISA treats premature action as a real risk: it can push an attacker to destroy evidence or accelerate impact.

[To be completed by Client Company]

Guidance drawn from: CISA Playbooks

27. Containment

> Short-term containment to stop the bleeding, then longer-term measures that let the business run while eradication is planned. Containment is a decision with costs on both sides — record what was accepted and who accepted it. Contain broadly enough that a partially-contained adversary cannot simply re-enter.

[To be completed by Client Company]

Guidance drawn from: CISA Playbooks; SANS; NIST SP 800-61r3

28. Eradication

> Removing the adversary and the conditions that let them in — not just the malware. CISA warns that a poorly orchestrated eradication lets an attacker hop back into cleaned areas, so eradication is planned and executed as one coordinated action rather than host by host over days. If new activity appears afterwards, contain and return to analysis.

[To be completed by Client Company]

Guidance drawn from: CISA Playbooks; SANS

29. Recovery and Return to Operations

> Restoring service on a known-good footing, in a stated order driven by business priority, with the monitoring you will apply afterwards and for how long. Say what "recovered" means and who declares it. Verify backups are reachable and clean before you depend on them.

[To be completed by Client Company]

Guidance drawn from: CISA Playbooks; SANS; NIST SP 800-61r3

30. Incident Workflow

> The whole sequence on one page, as a numbered flow from report through closure, with the decision points marked. This is the page to project during a tabletop.

[To be completed by Client Company]

Guidance drawn from: CISA Playbooks; ISP template

COMMUNICATIONS

31. Internal Communication and Notification

> Who is told what, when, and by whom — including the people who are not on the response team but whose work is affected. Say what staff are told and what they are asked not to do (forwarding, speculating publicly).

[To be completed by Client Company]

Guidance drawn from: CISA IRP Basics; ISP template

32. Communication Systems and Fallbacks

> The primary channel, the out-of-band fallback, and the trigger for switching. Name the specific tools and who can stand them up. Assume the primary is unavailable or untrusted.

[To be completed by Client Company]

Guidance drawn from: CISA IRP Basics; ISP template

33. Status Update Cadence

> How often each audience hears from you during an active incident, and from whom. A fixed cadence stops the response team being interrupted for updates and stops leadership inventing their own picture.

[To be completed by Client Company]

Guidance drawn from: ISP template; Zscaler

34. War Room and Response Environment

> Where the response runs, physical and virtual, and what has to be in it: displays, a shared timeline, the printed plan, the roster, and out-of-band comms. Include how remote participants join.

[To be completed by Client Company]

Guidance drawn from: ISP template

35. External Communication

> Customers, partners, press and social media — who speaks, who approves, and what the holding statement says. CISA recommends drafting press responses in advance: if a reporter calls claiming to have your data, the first minutes matter and a prepared holding statement buys them.

[To be completed by Client Company]

Guidance drawn from: CISA IRP Basics; Zscaler

36. Regulator and Government Notification

> Who files, to whom, on what clock, and who signs off. The Notification Obligations appendix lists the duties your jurisdiction, sector and data types trigger; this section says who executes them and how the evidence of filing is kept.

[To be completed by Client Company]

Guidance drawn from: NCIRP; NIST SP 800-61r3; ISP template

OUTSIDE HELP

37. Coordination with External Partners

> How you work with CISA, your sector ISAC, upstream providers and peers. The national plan organises federal support into four lines of effort — asset response (helping you recover), threat response (pursuing the actor), intelligence support, and affected-entity support — and knowing which one you are asking for makes the request faster.

[To be completed by Client Company]

Guidance drawn from: NCIRP; CISA Playbooks

38. Legal Counsel and Privilege

> When counsel is engaged and what runs under privilege. CISA advises reviewing this plan with an attorney before you need it — they may have strong preferences about how you engage outside responders and law enforcement, and those preferences are much cheaper to learn now.

[To be completed by Client Company]

Guidance drawn from: CISA IRP Basics

39. Law Enforcement Engagement

> Who your local law enforcement and FBI contacts are, and who decides to call them. Meet them before an incident: working out how to reach a field office is not something to do in the heat of battle, and law enforcement engagement is usually a decision taken with counsel.

[To be completed by Client Company]

Guidance drawn from: CISA IRP Basics; NCIRP

40. Outside Incident Response Support

> The firm you would call, the retainer or contract that makes them available, and who is authorised to trigger it. Select them in advance — negotiating a statement of work mid-incident costs the days you least have. Note what NIST calls the shared responsibility line: which parts of the response the provider owns and which stay yours.

[To be completed by Client Company]

Guidance drawn from: CISA IRP Basics; NIST SP 800-61r3; Zscaler

AFTER THE INCIDENT

41. Post-Incident Activity

> Closing the incident properly: final timeline, root cause, what was and was not determined, evidence disposition, and the report. NIST treats improvement as continuous rather than as a final phase — feed findings back into detection, controls and this plan.

[To be completed by Client Company]

Guidance drawn from: NIST SP 800-61r3; CISA Playbooks; SANS

42. Blameless Retrospective

> The meeting itself: who attends, how soon after closure, and the ground rule that makes it work. CISA is unambiguous — retrospectives must be blameless, or people stop contributing and the value is lost. Incidents are almost always a failure of the system rather than of one person, so examine people, process and technology, and focus on the process.

[To be completed by Client Company]

Guidance drawn from: CISA IRP Basics; SANS

43. Metrics and Reporting

> The handful of measures you actually track — time to detect, time to contain, incidents by category, recurrence — and who sees them. Choose measures that change a decision; drop the rest.

[To be completed by Client Company]

Guidance drawn from: NIST SP 800-61r3; Zscaler; ISP template

STAYING READY

44. Playbooks

> Per-incident-type procedures kept separately from this plan so they can change without reapproving the whole document. NIST notes that playbook formatting improves usability over prose — actionable steps, in order, for a specific scenario. List which playbooks exist and where they live.

[To be completed by Client Company]

Guidance drawn from: NIST SP 800-61r3; CISA Playbooks

45. Tabletop Exercises

> A facilitated role-play against a scenario, run on a stated cadence. CISA describes it plainly: the exercise might open with the communications lead receiving a reporter's email about rumours of a hack, and the facilitator injects updates to see how each role responds. Every sports team rehearses. Record the date, scenario, participants and the findings each exercise produced.

[To be completed by Client Company]

Guidance drawn from: CISA IRP Basics; NCIRP; Zscaler

46. Training and Validation

> What each role is trained on and how often, plus how procedures are validated. NIST recommends exercising documented procedures periodically both to confirm they still work and to train new people on them.

[To be completed by Client Company]

Guidance drawn from: NIST SP 800-61r3; Zscaler; ISP template

47. Response Toolkit (Jump Bag)

> The kit assembled in advance so responders are not sourcing tools mid-incident: bootable media with current anti-malware and forensic tools, write-blockers and clean storage, the printed contact list, spare devices, and known-good removable media. SANS keeps this as a standing checklist — inventory it on a schedule.

[To be completed by Client Company]

Guidance drawn from: SANS

48. Incident Log and Handler's Journal

> Contemporaneous notes with timestamps: who did what, where, why and how. SANS makes the standard explicit — every action taken by the response team is documented as it happens, because reconstructing it afterwards is unreliable and, if the matter reaches court, insufficient. Say where the journal lives and who reviews it.

[To be completed by Client Company]

Guidance drawn from: SANS; CISA Playbooks

49. Continuity and Failover

> How this plan meets your continuity and disaster recovery plans, and which failover paths have actually been tested. CISA recommends exercising full continuity of operations and failover systems rather than assuming they work; an untested restore is a hypothesis.

[To be completed by Client Company]

Guidance drawn from: CISA Playbooks; NIST SP 800-61r3

50. Supplier and Third-Party Incidents

> What happens when the incident is at a provider rather than in your environment: how you learn, what you can compel, and what you owe your own customers meanwhile. NIST treats supply-chain risk as a governance outcome; record notification terms and response obligations from the contracts themselves.

[To be completed by Client Company]

Guidance drawn from: NIST SP 800-61r3; Zscaler

51. Document Maintenance and Review

> Owner, review cadence, version history and approval. CISA recommends reviewing quarterly, on the grounds that the best plans are living documents that change with the business. Record what triggers an off-cycle review — a real incident, an exercise finding, a reorganisation.

Owned by the Director of Technology. Reviewed annually before the start of the school year, and after any Level 2 or Level 3 incident or any tabletop exercise. Material changes to process or authority require Superintendent approval.

Guidance drawn from: CISA IRP Basics; ISP template

52. Student Records and FERPA

> Which systems hold education records, who the records custodian is, and who may authorise disclosure to an outside responder during an investigation. Note the trap: FERPA governs access to those records but sets no breach-notification clock — the deadline that binds you is your state statute, listed in the Notification Obligations appendix. Treat the two as separate obligations.

Education records live in the student information system, the learning management system and the special-education case system. The records custodian is the Director of Student Services, who authorises any disclosure to an outside responder. FERPA governs that access but sets no breach-notification deadline; the clock that binds the district is the Nebraska breach statute in the Notification Obligations appendix.

Guidance drawn from: NIST SP 800-61r3; CISA IRP Basics

53. Instructional Continuity and Closure

> Who decides instruction cannot proceed, on what evidence, and how that decision reaches families and staff. Record the threshold for closing buildings versus running offline, what a paper day actually looks like, how many you can sustain, and any state reporting for lost instructional days.

The Superintendent decides whether instruction can proceed, on the recommendation of the Director of Technology. Buildings stay open and run offline wherever possible: paper attendance, paper lunch counts, printed rosters held in each office. The district can sustain three offline days before instructional-day reporting to the state is affected.

Guidance drawn from: CISA Playbooks; NIST SP 800-61r3

54. Family and Guardian Notification

> Who drafts, approves and sends notice to families, in which languages, and through what channel when the student information system and mass-notification tool may themselves be affected. Notice usually runs to the guardian; eligible students may hold that right themselves. Decide which before you need to send it.

[To be completed by Client Company]

Guidance drawn from: CISA IRP Basics

APPENDIX A

Sources and Attribution

The structure and guidance in this plan are synthesised from the public standards and guidance below. Each section cites the sources behind it. Nothing here reproduces those documents; consult them directly for their full text.

Incident Response Recommendations and Considerations for Cyber Risk Management

National Institute of Standards and Technology · NIST SP 800-61r3 · 2025-04

https://doi.org/10.6028/NIST.SP.800-61r3

Federal Government Cybersecurity Incident and Vulnerability Response Playbooks

Cybersecurity and Infrastructure Security Agency · CISA Playbooks · 2021-11

https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

Incident Response Plan (IRP) Basics

Cybersecurity and Infrastructure Security Agency · CISA IRP Basics · 2024-02

https://www.cisa.gov/resources-tools/resources/incident-response-plan-irp-basics

National Cyber Incident Response Plan (Update, Public Comment Draft)

Cybersecurity and Infrastructure Security Agency · NCIRP · 2024-12

https://www.cisa.gov/resources-tools/resources/national-cyber-incident-response-plan-ncirp

Incident Handler's Handbook

SANS Institute · SANS · 2011-12

https://www.sans.org/white-papers/33901/

Incident Response Readiness Guide

Zscaler · Zscaler · 2024

https://www.zscaler.com/resources/industry-reports/incident-response-readiness-guide.pdf

ISP Incident Response Plan (organisation template)

Contributed template · ISP template