Incident response plan template: Health care

Edition 16 November 2026. Free to copy and adapt under CC BY 4.0. Fields in [square brackets] are for you to fill in.

1. Purpose, scope and authority

This plan sets out how [Organization name] detects, declares, handles, recovers from and learns from cybersecurity incidents. It is written so that a person who has never handled an incident can act on it.

- Scope: this plan applies to [systems, sites, people, suppliers and data covered]. It does not cover [exclusions, for example physical safety emergencies handled under the site emergency plan].
- Owner: [Role, for example Chief Information Officer] owns this plan and keeps it current.
- Approval: [Role, for example Chief Executive Officer] approved version [number] on [date]. The next review is due on [date, no later than 12 months from approval].
- Definitions: an event is [any observable occurrence in a system or network]. An incident is an event or a set of events that has been declared against the criteria in section 5.
- Authority: the incident lead may isolate systems, disable accounts and take services offline as listed in section 7, without waiting for further approval.

2. Roles and responsibilities

Name one person and one deputy for each role. A role can be filled by an outside provider if the contract says so; write the provider name in the Name column.

Role	Name	Deputy	What this role decides
Executive sponsor	[name]	[name]	Funds the response. Approves shutting down or rebuilding critical services.
Incident lead	[name]	[name]	Declares and closes the incident. Sets priorities. Runs the response meetings.
Technical lead	[name]	[name]	Chooses containment and recovery actions. Directs system and network administrators.
Communications lead	[name]	[name]	Approves every internal and external message. Is the only spokesperson.
Legal and privacy lead	[name]	[name]	Decides which notice duties apply and when the clock started. Directs contact with regulators and law enforcement.
Human resources	[name]	[name]	Handles any case where an employee may be involved.
Facilities and physical security	[name]	[name]	Gives responders physical access to sites and devices.
System and data owners	[names]	[names]	Advise on recovery priority for their systems. Receive status updates.
Scribe	[name]	[name]	Keeps the incident log in appendix A.

Roles follow the examples in NIST SP 800-61 Rev. 3, section 2.2: leadership, incident handlers, technology professionals, legal, public affairs, human resources, physical security, and asset owners.

3. Contact and escalation sheet

Keep a printed copy and an offline copy. Use phone numbers that work if email and chat are down.

Who	Name or organization	Phone (24 hours)	Backup contact	Call when
Incident lead	[name]	[number]	[number]	Any suspected incident
Executive sponsor	[name]	[number]	[number]	Severity 3 or 4, or any legal duty to notify
Legal counsel	[firm or person]	[number]	[number]	Any exposure of personal data, or any contact with a regulator
Cyber insurer hotline	[insurer]	[number]	[policy number]	Before hiring outside responders, if the policy requires it
Incident response firm	[firm]	[number]	[retainer reference]	Severity 3 or 4, or when the team cannot scope the incident
Internet and cloud providers	[providers]	[numbers]	[account ids]	Attack on availability, or compromise of a cloud account
Law enforcement	[agency and office]	[number]		After legal counsel agrees, or when funds were sent
Regulators	[agency per section 10]	[number or portal]		As section 10 directs

4. Severity levels

Rate every incident on the same four-point scale as soon as it is declared, and re-rate it when facts change. Base the rating on business impact, not on how the attack looks.

Level	Criteria	Examples to adapt	Who is called	First response target
1 Low	One user or device. No sensitive data exposed. No service affected.	A blocked phishing email that no one opened.	Incident lead	[hours]
2 Medium	More than one user or device, or a non-critical service affected. No confirmed exposure of sensitive data.	One account compromised and reset before any data was accessed.	Incident lead, technical lead	[hours]
3 High	A critical service is down or degraded, or sensitive data may have been exposed.	Unauthorized access to a database holding customer records.	All roles in section 2, legal counsel	[minutes]
4 Critical	Wide loss of service, confirmed exposure of regulated data, or a threat to safety.	A compromised administrator account with access across the network.	All roles, executive sponsor, outside responders	[minutes]

Prioritizing by organizational impact, with a failed single workstation as minor and stolen privileged data as high, is the approach the SANS Incident Handler's Handbook describes.

5. Detecting, reporting and declaring an incident

Anyone who sees something unusual reports it. Only the incident lead, or the deputy, declares an incident.

- How staff report: [phone number], [email address] or [report button]. Reports are accepted at any hour. Staff are told in training that reporting a mistake will not be punished.
- Who receives reports: [role or team]. They log the report in appendix A within [15 minutes].
- Declaration criteria: declare an incident when an event shows [unauthorized access, loss or exposure of data, malicious software on a managed device, loss of a service caused by an attack, or a supplier report of any of these]. Add your own criteria.
- Out-of-band communication: if email or chat may be compromised, the team uses [phone bridge or secure messaging group] and tells affected users by phone.
- On declaration: the incident lead sets a severity (section 4), opens the log (appendix A) and starts the clock for every notice duty in section 10.

6. Triage and analysis

Work through these steps in order, and record each one in the log. Several can run at the same time.

1. Validate: confirm the report is real and not authorized activity such as an administrator running remote tools.
2. Scope: list the affected users, devices, accounts, services and data. Note what is not yet known.
3. Categorize: record the type, for example [phishing, malware, account compromise, data exposure, availability attack, insider, lost device, supplier].
4. Assess the data: state whether personal, regulated or confidential data may be involved, and whether it was encrypted.
5. Preserve evidence: before changing a system, capture logs and, where the technical lead decides it is needed, a memory and disk image.
6. Re-rate the severity and update the people called.

7. Containment

The aim is to stop the damage from spreading without destroying evidence or alerting the attacker more than needed. Record who approved each action and when.

Action	Who may approve	Business impact to weigh first	Logged where
Isolate a device from the network	[role]	[effect on users and services]	Appendix A
Disable or reset an account	[role]	[effect on the person and linked services]	Appendix A
Block an address, domain or file	[role]	[effect on legitimate traffic]	Appendix A
Take a service offline	[role]	[customers and contracts affected]	Appendix A
Rotate keys and service account secrets	[role]	[systems that will fail until updated]	Appendix A

Short-term containment limits damage fast. Long-term containment keeps systems in production safely while a rebuild is prepared. Take a backup image of an affected system before wiping it.

8. Eradication and recovery

Do not start removal until every known way back in has been found and the evidence is collected. Do not declare recovery until the checks below pass.

1. Confirm containment: no new signs of attacker activity for [period].
2. Eradicate: remove malicious files, close the entry point, reset affected credentials, patch the exploited weakness, and rebuild systems from known-good sources where there is doubt.
3. Verify backups before restoring from them, and restore to clean systems only.
4. Test restored systems, then watch them closely for [period] for signs of re-entry.
5. Declare the end of recovery: the incident lead signs when the exit criteria are met: [criteria, for example services at normal levels, no alerts for 72 hours, owners agree].

9. Communications

One person speaks for the organization. Facts are confirmed before they are shared, and nothing is guessed in writing.

Audience	Owner	Channel	Approved by	Timing
Employees	[role]	[channel]	Communications lead	[when]
Customers and partners	[role]	[channel]	Communications lead, legal	[when]
Regulators and law enforcement	Legal and privacy lead	[portal or phone]	Legal and privacy lead	As section 10 directs
Insurer	[role]	[hotline]	Executive sponsor	[when]
Media	Communications lead	Holding statement	Executive sponsor, legal	Only if asked or required
Executives and board	Incident lead	[channel]	Incident lead	[interval]

Prepare a holding statement now: "We are investigating a security incident. We will share confirmed facts as we have them. Contact [name and number] with questions."

10. Legal, regulatory, contractual and insurance notices

List every duty to notify that applies to your organization, with the trigger, the deadline and the owner. The legal and privacy lead confirms the list at least once a year. Record the date and time each clock started.

Rule, contract or policy	Applies when	Deadline and to whom	Owner	Source
[Name the law, for example a state breach notification law]	[trigger]	[deadline] to [authority or individuals]	[role]	[link]
[Customer contract clause]	[trigger]	[deadline] to [customer]	[role]	[contract reference]
[Cyber insurance policy]	[trigger]	[deadline] to [insurer]	[role]	[policy number]
[Other]	[trigger]	[deadline]	[role]	[link]

The company-type pages of this site show the filled-in rows for health care, financial services, public companies, software providers, schools, federal agencies and the United Kingdom, each with its source.

10A. Health care: HIPAA breach notification

Use this addendum if your organization is a HIPAA covered entity or a business associate. It adds the notice duties of the HIPAA Breach Notification Rule to section 10.

- Record the date and time of discovery in the incident log, because the 60-day period counts from it.
- Record whether the data was encrypted to the standard that makes it "secured". Only unsecured protected health information triggers these notices.
- The individual notice must include: what happened with dates, the types of information involved, steps individuals should take, what the entity is doing, and contact procedures that include a toll-free number, an email address, a website or a postal address (164.404(c)).
- A business associate adds the covered entity's incident contact to the contact sheet and the time allowed by the contract, which may be shorter than 60 days.

Duty	What the rule says	Deadline	Source
Presumption of breach	An impermissible use or sharing of protected health information is presumed a breach unless a risk assessment shows a low probability of compromise. The assessment weighs four factors: the nature and extent of the information, the person who used or received it, whether it was actually acquired or viewed, and how far the risk was mitigated.	Decide before the notice clock questions arise	45 CFR 164.402
Notice to individuals	Notify each individual affected by a breach of unsecured protected health information, in plain language, by first-class mail or by email if the person agreed.	Without unreasonable delay and no later than 60 calendar days after discovery	45 CFR 164.404
When a breach is "discovered"	The first day the breach is known, or would have been known with reasonable diligence, to the covered entity.	Start the clock on that day	45 CFR 164.404(a)(2)
Notice to the Secretary of HHS	500 or more individuals: notify at the same time as individuals. Fewer than 500: keep a log and notify within 60 days after the end of the calendar year.	Same time, or 60 days after year end	45 CFR 164.408
Notice to media	More than 500 residents of a State or jurisdiction: notify prominent media outlets serving that area.	No later than 60 calendar days after discovery	45 CFR 164.406
Business associate to covered entity	A business associate notifies the covered entity of a breach it discovers.	Without unreasonable delay and no later than 60 calendar days after discovery	45 CFR 164.410

11. Evidence handling and documentation

Write down what happened, what was decided, and by whom, at the time. The log supports the review, regulators, insurers and any later legal action.

- Record for each entry: date and time with time zone, who observed or acted, what was seen or done, which system, where evidence is stored.

- Store logs, images and notes in a location only responders can reach.
- For each evidence item record: item id, source, who collected it, when, how it was copied, a hash value if available, and who has handled it since.
- Do not edit entries after the fact. Add a correction as a new entry.

12. Third parties and suppliers

List the providers who hold your data or run your systems, and what each must tell you and when. Include them in exercises.

Third party	Service	Incident contact	Their duty to tell us	Our duty to tell them
[provider]	[service]	[name and number]	[contract clause and time]	[when]
[provider]	[service]	[name and number]	[contract clause and time]	[when]

Check what each provider may do on your behalf during an incident, such as shutting off a service, and what it may not share with its other customers.

13. Post-incident review

Hold a review after every declared incident, as soon as possible and within [10 business days] of closing it. Keep the meeting short and about facts and fixes, not blame.

- Agenda: what happened and when; what worked; what did not; what was missing, including information that was hard to get.
- Outputs: a closing report (appendix D), the root cause, and a list of actions each with an owner and a due date.
- Update this plan, the contact sheet and the detections within [30 days].
- Share what was learned with the people who need it, without waiting for the final report if a lesson is urgent.

14. Testing, training and keeping the plan current

A plan that has not been practiced is a draft.

- Exercise: walk through this plan with all roles at least once every [12 months] using a realistic scenario, and record the findings.
- Test restoring critical systems from backups at least once every [12 months].
- Training: every responder is trained for their role. All staff learn how to report an incident.
- Distribution: current copies are available to every person with a role, including offline, and are reachable during an incident.
- Update this plan when roles change, after every incident or exercise, and when a law or contract changes a notice duty.

Appendices: forms

Copy these forms into your records system. Appendix A is opened on declaration and closed on review.

Appendix	Form	Fields
A	Incident log	Entry number; date and time; recorded by; what was observed or done; system; evidence id; decision and approver
B	Timeline	Time of first malicious activity; time detected; time declared; time contained; time notices sent; time recovered; time closed
C	Handover note	Current status; open actions; next decisions; people on shift; next update time; where the log is
D	Closing report	Summary; cause; impact; data involved; notices sent with times; cost; lessons; actions with owners and dates