Data Breach Response Procedure

SOP · US · Updated 2026-07-13 · Square brackets are placeholders to replace with your own details.

A data breach response procedure is the written sequence your team follows when personal information is lost, stolen, sent to the wrong person, or accessed without authorization — who to tell first, how to contain the damage, how to assess what was exposed and about whom, and how to work out which notification laws apply. It is the difference between a response and a scramble.

The US has no single breach notification law. Every state — plus the District of Columbia and US territories — has its own, and they differ on what counts as personal information, who gets notified, and how quickly. The one thing they share is that the clock generally starts at discovery, which is why the roles, the reporting channel, and the assessment steps in this procedure are decided in advance — you cannot design a response during a live incident.

This template follows the shape of the FTC's data breach response guidance — secure, fix, notify — and gives you the full procedure: what counts as a breach, immediate containment, the scope and risk assessment, the state-by-state notification check, telling the people affected, and the breach log that evidences it all.

Purpose and scope

This procedure sets out how [Your company] responds to actual or suspected breaches of personal information. It applies to all staff, all systems, and all personal information we hold — about customers, staff, or anyone else — in any format.

What counts as a data breach

- An email, letter, or attachment containing personal information sent to the wrong recipient.
- A lost or stolen laptop, phone, USB drive, or paper file.
- A phishing compromise, ransomware infection, or other unauthorized access to systems holding personal information.
- Staff accessing records they have no work reason to see.
- A vendor or service provider telling us their systems holding our data were compromised.
- If in doubt, report it — the assessment below decides whether it matters, not the person who spotted it.

Roles and responsibilities

- Breach lead ([name/role], deputy [name/role]): runs the response, owns the breach log, and makes notification decisions with [senior role] and counsel.
- IT support ([name/provider]): contains technical incidents and preserves evidence.
- Legal counsel ([firm/contact]): advises on which state laws apply and reviews notification content before anything is sent.

- All staff: report suspected breaches immediately by [phone number/channel]. Honest mistakes reported promptly are never treated as misconduct; concealment is.

Immediate actions: report and contain

1. Report the suspected breach to the breach lead at once by [phone/channel] — including evenings and weekends. Do not wait for the next business day.
2. Record the date and time of discovery precisely — notification clocks in most state laws run from around this point, and the record will be examined.
3. Contain the breach: recall the email, remote-wipe the device, disable compromised accounts and change passwords, isolate affected systems, or retrieve the papers — whichever applies. Take affected equipment offline, but do not turn machines off until forensic advice says so.
4. Preserve evidence. Do not delete emails, logs, or files connected to the incident.
5. Notify your cyber insurer [policy/contact] before engaging outside help — many policies have their own notice conditions and approved forensic and legal vendors.
6. Ask any unintended recipient to delete the information and confirm in writing that they have.

Assess the scope and the risk

1. Establish the facts: what happened, which systems and records were involved, and whether the exposure is ongoing.
2. Identify the data elements exposed — names, Social Security numbers, driver's license numbers, financial account or card details, health information, login credentials — because state laws define "personal information" by combinations of exactly these elements.
3. Identify whose information it is and, critically, which states and territories they live in — that list determines which notification laws apply.
4. Assess the likelihood and severity of harm: identity theft, financial fraud, account takeover, physical risk, or distress; weight the assessment up where children's data or credentials are involved.
5. Record the assessment and conclusions in the breach log, however minor the incident turns out to be.

Notification: check every state that applies

There is no single US notification deadline to rely on — the deadlines, formats, and recipients differ by state. Using the state list from the assessment, [name/role] and counsel check the current requirements of each affected state attorney general: whether the incident meets that state's definition of a breach, whether encrypted data is exempt, who is notified and how, whether the AG or state agencies are notified directly, and whether consumer reporting agencies come into scope at that state's threshold. Work from the state AG pages and current counsel advice, not from templates or last year's memory.

Consider law enforcement early: the FTC's guide covers when to involve local police or federal agencies, and a law enforcement request can affect notification timing. If the decision in any state is that notification is not required, record the reasoning in the breach log — that record is what shows the decision was considered, not missed.

Telling the people affected

Where notification is required — or is simply the right call — tell people in plain language: what happened, what information was involved, what we are doing, what they can do to protect themselves, and who to contact at [Your company]. The FTC's guide includes a model letter, and IdentityTheft.gov is the standard resource to point people to for recovery steps. Some state laws prescribe specific content for the notice, so counsel reviews it before it goes out.

Coordinate with [insurer/forensics/law enforcement] before communicating, but do not let coordination become delay — the clock does not pause while the message is polished.

Records, lessons, and review

Every breach and near miss goes in the breach log kept at [system/location]: dates and times, facts, assessment, state-by-state decisions, notifications, and actions. Within [period] of closing an incident, the breach lead runs a lessons-learned review and feeds the fixes into training, systems, vendor contracts, and this procedure.

This procedure is reviewed [frequency, e.g. annually] and after every notifiable incident — and the state-law landscape shifts often enough that the review should include a fresh check of the states where your customers live. Owner: [name/role]. Next review due: [date].

How to use this template

1. Name the breach lead and deputy, and put their out-of-hours contact details where staff will actually find them at 6 p.m. on a Friday.
2. Brief every team that the rule is "report at once, blame later" — the procedure fails if staff sit on mistakes.
3. Line up counsel and check your cyber insurance conditions now: many policies dictate the first phone call, and mid-incident is the wrong time to discover that.
4. List the states where your customers and staff live and bookmark each state AG's breach guidance — that list is your notification map.
5. Check your vendor and software contracts require prompt breach notice to you — their breach becomes your notification duty.
6. Run a tabletop exercise on a realistic scenario — a stolen laptop or a phished mailbox — within a month of adopting the procedure.

Official guidance

› FTC — Data Breach Response: A Guide for Business

- FTC — Protecting Personal Information: A Guide for Business
- FTC — Privacy and security business guidance