Vendor incident response checklist

When a vendor has a breach or an outage, the incident is theirs and the consequences are yours. Your customers and your regulators will look to you. This checklist covers what to do from the first notice through resolution, and what to record so the response can be shown afterward.

Vendor _____ Completed by _____ Date _____

In the first hours

- [ ] The notice is logged with the date and time it arrived and who received it.
- [ ] One person at your institution owns the incident, and the vendor knows who it is.
- [ ] You have confirmed what happened, when it started and whether it is still going on.
- [ ] You know which of your systems, data and customers are involved, or have asked.
- [ ] Access between the vendor and your systems is limited or shut off if the incident could spread.
- [ ] Your own incident response team, information security and management are told.

Understand the impact

- [ ] The vendor has said in writing what data was affected and how many records.
- [ ] You have compared the vendor's account with what your own logs show.
- [ ] You know whether the service is degraded or down and what the workaround is.
- [ ] The vendor's subcontractors are accounted for, if the incident began with one of them.
- [ ] The incident is classified by type and severity under your own policy.

Meet your obligations

Notification duties depend on the data, the law and your contracts. Involve counsel before deciding who must be told.

- [ ] Counsel has advised on which laws and regulations require notice, and by when.
- [ ] Regulators are notified where required, within the time allowed.
- [ ] Affected customers are notified where required, with wording counsel has approved.

- [ ] Your cyber insurer is notified as your policy requires.
- [ ] The contract has been checked for the vendor's notification, cooperation and cost obligations.

Get the vendor's formal response

- [ ] The vendor has given a written account of the cause.
- [ ] The vendor has described what it did to contain the incident.
- [ ] The vendor has committed to corrective actions with dates.
- [ ] Updates arrive on an agreed schedule until the incident is closed.

Resolve and verify

- [ ] The service is restored and your own team has confirmed it.
- [ ] Each corrective action is tracked to completion and checked, not only reported as done.
- [ ] Evidence of the fix is on file, such as a test result or an updated report.
- [ ] The date of resolution and the time it took are recorded.
- [ ] You have recorded whether the vendor met the contract's terms for response and resolution.

Afterward

- [ ] A short written review covers what happened, what worked and what did not.
- [ ] The vendor's risk level is reassessed in light of the incident.
- [ ] Due diligence is brought forward if the incident exposed a weakness in the vendor's controls.
- [ ] Service credits or other remedies in the contract are claimed.
- [ ] Changes to the contract are noted for the next renewal.
- [ ] The incident is included in reporting to management and the board.

Questions to put to the vendor

Question	Why it matters
What happened and when did it start?	Sets the window you must check on your side
When did you discover it?	Shows how long it went unnoticed and whether notice to you was timely
Which of our data and systems were affected?	Decides your own notification duties
Is it contained?	Tells you whether to cut access now
What was the cause?	Shows whether the same thing can happen again
What are you changing and by when?	Gives you corrective actions to track
Who else have you notified?	Regulators and the press may contact you next

A free checklist from VendorRisk, vendor management software for regulated institutions. More guides, checklists and templates at vendorrisk.com/resources.