Incident Response Communications Guide

When a security incident happens, the reporting clock may already be running. Teams should establish their communications, escalation paths, and responsibilities before they need them.

WHAT IS INSIDE

PART 01

Internal incident response SOP

Twelve steps from identification through post incident review, including severity, evidence, containment, reporting assessment, and closure.

PART 02

Customer notification email

A ready to adapt notification built on the known, unknown, and doing structure, with a short holding statement for the first hours.

PART 03

Quick checklist and contacts

A single page to work from under pressure, plus the contact block that should be filled in and kept current.

HOW TO USE IT

Work through it once before you need it. Assign the roles, agree the severity model, confirm who signs external messages, and get the notification language reviewed by legal and communications while nothing is on fire. Store the completed version where responders can reach it without production access.

Fields shown in [brackets] are the decisions your organization owns. Everything else is ready to use as written.

WHO IT IS FOR

- CISOs and security leaders
- SaaS and software companies
- Engineering and security teams
- North American vendors selling into the EU

Regulatory classification and notification decisions should involve qualified legal and compliance personnel. This guide is an operational template, not legal advice.

Internal standard operating procedure

This procedure establishes how [Company] identifies, investigates, escalates, remediates, documents, and communicates potential cybersecurity incidents.

It exists so that technical investigation, business decision making, regulatory assessment, and customer communication can happen in parallel and at speed. Adapt it to your systems, legal obligations, contractual commitments, and response structure.

DOCUMENT CONTROL

Owner	[Security / CISO]
Version	[Version]
Reviewed	[Date]
Next review	[Date]

01 Incident identified

Open an incident record and notify the designated incident response lead. Do not wait for complete information before opening an incident.

AN INCIDENT MAY SURFACE THROUGH

- Security monitoring or alerts
- Employee, customer, or vendor reports
- Vulnerability disclosure
- Penetration testing or security testing
- Threat intelligence
- Law enforcement or regulatory notification
- Evidence of active exploitation

RECORD IMMEDIATELY

- Date and time discovered
- How the issue was discovered
- Person or system that identified it
- Affected or potentially affected systems
- Known indicators and initial evidence
- Actions already taken

02 Assign an incident lead

One person coordinates the response and maintains the record of decisions and actions, even when several teams are involved. Incident lead: [Role / name] Backup: [Role / name]

FUNCTION	PRIMARY RESPONSIBILITY
Security	Investigation, evidence, containment, and security assessment
Engineering	Product analysis, remediation, testing, and deployment
Legal and compliance	Regulatory, legal, and contractual assessment
Executive leadership	Business decisions and executive escalation
Communications	External messaging and communications coordination
Customer success and support	Customer communication and inbound questions

03 Triage and classify

ESTABLISH AS QUICKLY AS POSSIBLE

- What happened, and when did it begin?
- Is exploitation suspected or confirmed?
- Is the incident ongoing?
- Which systems, products, or versions are affected?
- Which customers may be affected?
- Could data have been accessed, modified, destroyed, or disclosed?
- Is product functionality or availability affected?
- Is a third party component involved?
- What evidence is available now?
- What is still unknown?

SEV-1 CRITICAL

Confirmed or highly likely significant compromise, active exploitation, or major customer, product, or business impact.

SEV-2 HIGH

Significant security issue requiring urgent investigation, with limited or unconfirmed impact.

SEV-3 MEDIUM

Security issue requiring investigation with limited immediate impact.

SEV-4 LOW

Low risk event that can follow normal security workflows.

Replace these definitions with your established severity model where one exists. What matters is that the level maps to a known escalation path, not that the labels match.

04 Preserve evidence

Preserve what will be needed to reconstruct the incident, and avoid unnecessarily altering or destroying it during containment and remediation. Record significant vulnerabilities and decisions with timestamps as you go.

- Application and API logs
- Authentication and identity logs
- Cloud audit logs
- SIEM events

- Endpoint telemetry
- Network logs
- Source code and deployment records
- CI/CD records
- Vulnerability scanner results
- Affected component versions
- Third party notifications
- Relevant internal communications

05 Contain the incident

Security and engineering weigh the risk of continued exploitation against the operational impact of each action. Document what changed, when, who approved it, and why.

- Disable compromised accounts
- Rotate credentials, keys, or tokens
- Isolate affected systems
- Disable vulnerable functionality
- Block indicators of compromise
- Apply temporary mitigations
- Restrict access
- Increase monitoring
- Withdraw affected releases

06 Determine reporting and notification obligations

Escalate potentially reportable incidents to legal, compliance, and security decision makers immediately. This is the step where the clock matters most.

ASSESS WHETHER THE INCIDENT TRIGGERS

- Applicable cybersecurity regulations
- Data breach or privacy notification requirements
- Customer contract commitments
- Cyber insurance requirements
- Partner or vendor obligations

RECORD FOR EVERY REPORTABLE EVENT

- Time the organization became aware
- Reporting assessment and decision
- Decision makers and rationale
- Applicable deadlines and submission owner
- Confirmation of submission

07 Establish a communications plan

Decide which audiences require communication, and designate one owner for external messaging. Candidate audiences: regulators, affected customers, employees, executive leadership, the board, the cyber insurer, vendors and partners, law enforcement, and the general public or media.

What we know

Facts supported by current evidence. Nothing inferred, nothing assumed.

What we do not yet know

Open questions still under investigation, stated plainly rather than omitted.

What we are doing

Containment, investigation, remediation, and customer protection measures underway.

Never present assumptions as confirmed facts. Where information is incomplete, say explicitly that the investigation is ongoing.

08 Notify affected customers

Where notification is required or appropriate, start from the customer notification template in Part 02. Security, legal, and communications review external incident communications according to your approval process. Do not delay urgent escalation because final customer wording is not yet approved.

- What happened, and when it was identified
- What is currently known
- Products or services potentially affected
- Potential customer impact
- Actions the company has taken
- Actions customers should take, if any
- When customers can expect another update
- Where customers can ask questions

09 Remediate and validate

Once the root cause is understood: develop the remediation, review the proposed fix, test it, and validate that the vulnerability can no longer be exploited. Check for related attack paths and similar vulnerabilities elsewhere, deploy, and monitor for continued exploitation.

Where appropriate, use targeted security testing or penetration testing to confirm that the remediation addresses the underlying vulnerability rather than only its visible symptoms. Then determine whether affected customers need additional instructions.

10 Maintain a single incident timeline

One authoritative timeline, maintained throughout, so the organization can reconstruct what happened, what was decided, and when.

Initial activity | Detection | Internal escalation | Major vulnerabilities | Containment | Reporting decision | Regulatory notification | Customer communication | Remediation | Validation | Closure

11 Close the incident

The incident lead approves closure, and only once every condition below is true.

- Immediate security risk has been addressed
- Remediation is complete or formally tracked
- Required notifications have been made
- Customer commitments are complete or assigned
- Relevant monitoring remains in place
- Evidence and documentation have been retained

Closure date: [Date] Approved by: [Name / role]

12 Conduct a post incident review

Schedule the review within five to ten business days of closure for significant incidents. Assign every improvement an owner and a target completion date.

- What allowed the incident to occur?
- What allowed us to detect it, and what delayed detection?
- Did we have sufficient logs and telemetry?
- Did responders have the access they needed?
- Were responsibilities and escalation paths clear?
- Could we identify affected products and customers quickly?
- Were communications timely and accurate?
- Did our security controls behave as expected?
- What would have happened at greater severity?
- Where did the response process break down?

Customer security incident notification

Send this once the facts in it are true, and not before. The structure is deliberate: customers need to know what is confirmed, what is still open, what you are doing, and when they will hear from you again. Anything else can wait for the next update.

SUBJECT [Security Incident Update] Important information regarding [Product / Service]

Dear [Customer name],

We are writing to inform you of a security incident that may affect your use of [Product / Service]. We want you to have the facts we have today, what we are still working to confirm, and the steps we are taking.

WHAT HAPPENED

On [date], our security team identified [factual description of the issue] affecting [system, product, or component]. We began investigating immediately and [contained the issue by / are actively containing the issue by].

WHAT WE KNOW

Based on our investigation to date: [confirmed facts, including the period of exposure and the data or functionality involved]. We have no evidence at this time that [state only what the evidence actually supports].

WHAT WE DO NOT YET KNOW

Our investigation is ongoing. We are still working to determine [open questions]. We will not speculate ahead of the evidence, and we will tell you what we find.

WHAT WE ARE DOING

We have [containment and remediation actions taken]. We are [investigation, monitoring, and validation work underway], and we have engaged [external support, if applicable].

WHAT WE RECOMMEND YOU DO

[Specific customer actions, or: no action is required from you at this time.] If you would like to review activity on your own account, [how to do that].

NEXT UPDATE

We will provide our next update by [date and time, with time zone], whether or not there is new information to report. If you have questions in the meantime, contact us at [security contact address].

We take the security of your data seriously, and we are treating this with the urgency it deserves.

[Name]
[Title], [Company]

HOLDING STATEMENT, FIRST HOURS

Use when customers are asking and the investigation is too young to answer them.

> We are aware of a potential security issue affecting [Product / Service] and our security team is actively investigating. We are treating it as our highest priority. We will share confirmed information, including any impact to your account, by [date and time]. We would rather be accurate than fast, and we will not speculate while the investigation is open.

Quick checklist and key contacts

PRINT AND KEEP WORKING PAGE

Sequence matters less than coverage. Work down the list, note the time against each item, and hand the page to whoever takes over from you.

- [ ] Open the incident record and note the discovery time
- [ ] Assign the incident lead
- [ ] Determine initial severity
- [ ] Identify affected or potentially affected products and systems
- [ ] Preserve relevant evidence
- [ ] Determine whether exploitation is active
- [ ] Begin containment
- [ ] Notify required internal stakeholders
- [ ] Escalate potential reporting obligations to legal and compliance
- [ ] Record regulatory and contractual deadlines
- [ ] Establish what is known, unknown, and under investigation
- [ ] Determine whether customers require notification
- [ ] Prepare and approve the customer communication
- [ ] Remediate the identified vulnerability
- [ ] Validate the remediation independently
- [ ] Continue monitoring
- [ ] Maintain the incident timeline
- [ ] Complete required follow up communications
- [ ] Conduct the post incident review
- [ ] Assign and track improvement actions

KEY CONTACTS

Incident lead
[Name / phone / email]

Security
[Contact]

Engineering
[Contact]

Legal and compliance
[Contact]

Executive escalation
[Contact]

Communications
[Contact]

Customer support
[Contact]

Cyber insurer
[Contact]

External IR provider
[Contact]

This guide supports incident response planning and communications. Organizations should adapt it to their own environment and have qualified legal and compliance professionals determine applicable notification and reporting obligations. Software Secured is a Canadian manual penetration testing firm; validation testing after remediation is one of the places an independent team is most useful.