

Security Incident Response Plan

Use this template to response plan for cybersecurity incidents and breaches.

Template Metadata

Field	Details
Category	Cybersecurity & Privacy
Owner	[Team or owner]
Version	[Version number]
Effective Date	[Date]
Review Cycle	[Monthly / Quarterly / Annual / Event-based]
Status	[Draft / In Review / Approved]

Incident Classification

Define severity levels, examples, and declaration criteria.

Item	Details	Owner	Status
[Item or requirement]	[Describe the relevant detail, evidence, or decision]	[Owner]	[Open / Complete]
[Item or requirement]	[Describe the relevant detail, evidence, or decision]	[Owner]	[Open / Complete]

Notes

[Add context, assumptions, exceptions, evidence links, screenshots, calculations, or reviewer comments.]

Roles

Assign incident commander, security lead, communications, legal, and engineering owners.

Item	Details	Owner	Status
[Item or requirement]	[Describe the relevant detail, evidence, or decision]	[Owner]	[Open / Complete]
[Item or requirement]	[Describe the relevant detail, evidence, or decision]	[Owner]	[Open / Complete]

Notes

[Add context, assumptions, exceptions, evidence links, screenshots, calculations, or reviewer comments.]

Containment

List immediate steps to limit exposure and preserve evidence.

Item	Details	Owner	Status
[Item or requirement]	[Describe the relevant detail, evidence, or decision]	[Owner]	[Open / Complete]
[Item or requirement]	[Describe the relevant detail, evidence, or decision]	[Owner]	[Open / Complete]

Notes

[Add context, assumptions, exceptions, evidence links, screenshots, calculations, or reviewer comments.]

Investigation

Describe evidence collection, log review, timeline building, and root cause analysis.

Item	Details	Owner	Status
[Item or requirement]	[Describe the relevant detail, evidence, or decision]	[Owner]	[Open / Complete]
[Item or requirement]	[Describe the relevant detail, evidence, or decision]	[Owner]	[Open / Complete]

Notes

[Add context, assumptions, exceptions, evidence links, screenshots, calculations, or reviewer comments.]

Notifications

Define internal, customer, regulator, insurer, and law enforcement notification paths.

Item	Details	Owner	Status
[Item or requirement]	[Describe the relevant detail, evidence, or decision]	[Owner]	[Open / Complete]
[Item or requirement]	[Describe the relevant detail, evidence, or decision]	[Owner]	[Open / Complete]

Notes

[Add context, assumptions, exceptions, evidence links, screenshots, calculations, or reviewer comments.]

Recovery

Specify restoration, monitoring, validation, and customer confirmation steps.

Item	Details	Owner	Status
[Item or requirement]	[Describe the relevant detail, evidence, or decision]	[Owner]	[Open / Complete]
[Item or requirement]	[Describe the relevant detail, evidence, or decision]	[Owner]	[Open / Complete]

Notes

[Add context, assumptions, exceptions, evidence links, screenshots, calculations, or reviewer comments.]

Postmortem

Include lessons learned, corrective actions, and evidence retention. Use time-bound actions and avoid speculative language.

Item	Details	Owner	Status
[Item or requirement]	[Describe the relevant detail, evidence, or decision]	[Owner]	[Open / Complete]
[Item or requirement]	[Describe the relevant detail, evidence, or decision]	[Owner]	[Open / Complete]

Notes

[Add context, assumptions, exceptions, evidence links, screenshots, calculations, or reviewer comments.]

Review and Signoff

Document review conclusions, approvals, unresolved items, and next review date.

Role	Name	Date	Notes
Preparer	[Name]	[Date]	[Notes]
Reviewer	[Name]	[Date]	[Notes]
Approver	[Name]	[Date]	[Notes]