Incident Response Playbook

Actionable guide for how to report events, define responsibilities, and manage response procedures
Checklist

3 About This Playbook

3 New Incident

3 Responsibilities and Procedures (ISO 27001 – Annex A 16.1.1)

3 Reporting Information Security Events (ISO 27001 – Annex A 16.1.2)

3 Detection & Reporting Information Security Weaknesses (ISO 27001 – Annex A 16.1.3)

3 Assessment and Decision on Information Security Events (ISO 27001 – Annex A 16.1.4)

5 Investigating

5 Receiving the Report and Assessing the Cause and Type of Breach (ISO 27001 – Annex A 16.1.5)

6 Incident Response Team Initial Responsibilities

7 Remediating

7 Containment Strategy

7 Collection of Evidence (ISO 27001 – Annex A 16.1.7)

8 Forensic Analysis

8 Retention of Evidence

9 Notifying

9 Communication/Disclosure Strategy

9 Assessment of Incidents for Legal Reporting

10 Notification Process

10 Notification Details:

11 Complete

11 Learning from Information Security Incidents (ISO 27001 – Annex A 16.1.6)

DISCLAIMER

No part of this document may be reproduced in any form without the written permission of the copyright owner.

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. OneTrust LLC shall have no liability for any error or damage of any kind resulting from the use of this document.

OneTrust products, content and materials are for informational purposes only and not for the purpose of providing legal advice. You should contact your attorney to obtain advice with respect to any particular issue. OneTrust materials do not guarantee compliance with applicable laws and regulations.

Copyright © 2018 OneTrust LLC. All rights reserved. Proprietary & Confidential.
About This Playbook

This playbook provides a framework for reporting events and weaknesses, defining responsibilities, response procedures and collection of evidence. It can provide the oversight of and guidance for the required processes for an organisation’s privacy and data security incident and breach response in compliance with federal and state privacy and data protection laws. The organisation of this document is designed to address key controls required by ISO 27001 as well as obligations that are common throughout global legal requirements.

New Incident

✅ **Responsibilities and Procedures (ISO 27001 – Annex A 16.1.1)**

It is left to the judgment of the responding member of the Incident Response Team (IRT), or their designee, to determine when to convene the Incident Response Team, however, it will generally be necessary for all “significant” incidents which are incidents with a “medium” or “high” severity. If an IRT is convened, this playbook should be consulted, and the elements appropriate to the individual incident should be followed.


Define and list the minimum required individuals or functional areas for the IRT for every incident for which the IRT is convened (smaller incidents will likely be handled by privacy and security teams). Additionally, define the other functions that will be called upon as appropriate for the incident such as the head of Human Resources or Public Relations.


**Detection Mechanisms**

- Notification of incident from internal logging/audit controls
- Internal automated report of anomalous system utilization or outage

**Reports**

- Report of incident from client/customer
- Report of potential compromise from 3rd party
• All workforce personnel are required to report any suspicious activity (by others or by systems) immediately.
  1. Send an email (and call if there is no response within 20 minutes) to example@company.com
  2. An incident report should be completed as soon as possible by the reporter employee. Ideally this is done within an application like OneTrust Privacy Management Software which will track and assist with the end to end workflow.

✓ Assessment and Decision on Information Security Events (ISO 27001 – Annex A 16.1.4)

Security or privacy incident examples include the presence of a malicious application, such as a virus; establishment of an unauthorised account for a computer or application; unauthorized network activity; presence of unexpected/unusual programs; computer theft; failure to adequately destroy protected information such as failure to shred paper or securely erase data; accessing protected information not required for one’s job; releasing more protected information than is necessary for the given purpose; sharing passwords; failure to log off a system or our network and leaving a workstation unattended; and more. OneTrust Privacy Management Software is used for reporting and reviewing events and incidents, and for determining whether legal or contractual obligations have been triggered (e.g., breach notification). The template questionnaires are designed to assist with global personal data breach obligations.

Part 1 should be completed by the business user who is reporting the incident, and then be submitted for review. Part 1 includes questions about the following:

1. Cause of the incident
2. Networks involved
3. Assets involved
4. Clients/vendors involved
5. Data compromised
6. Categories of individuals affected by the incident
7. Number of individuals affected
8. Number of data records compromised
9. Review of data risk
10. Prior public availability of the data
11. Use of encryption
12. Details about person/people who received the data
13. If the data was actually viewed or acquired
14. To what extent has the risk to the data already been mitigated
15. Technical or organisational protection measures already implemented and applied
16. Any subsequent measures taken
17. Evidence collected

Part 2 should be completed by the Privacy/Security lead or his/her designee, after Part 1 has been submitted and reviewed. Generally, it is only required where it has been determined that a “personal data breach” has occurred but may be used for lesser events/incidents as needed. Part 2 includes questions about the following:

1. Organisation's relationship to the data (i.e., controller vs processor);
2. The level of risk to natural persons created by the breach;
3. The likely consequences of the breach;
4. Mitigation plans;
5. The personnel involved in the response; and
6. Any contracts affected by the breach (e.g., customers or vendors).
Investigating

**Receiving the Report and Assessing the Cause and Type of Breach (ISO 27001 – Annex A 16.1.5)**

1. Review Part 1 and Part 2 Assessments
2. Correlate and analyse collected logs to determine criticality
   a. Gateway logs
   b. Infrastructure logs
   c. Host audit logs
   d. Database audit logs
   e. Network watcher for network traffic logs
   f. Depending on type of compromise, consider additional logs to be collected
3. Depending on the documentation provided to the IRT, it should either validate or determine what types of data are involved (e.g., personal data), which identifiers were involved, whether the data was encrypted (and the method / strength of encryption), adequacy of password security, the type of incident, and whether logging was active and adequate. It is particularly important to validate information provided to the IRT, as some breaches have initially overlooked personal data. The cause of the breach is determined by technical analysis and investigation.
4. If the responding member of the IRT scores the incident as “high” severity, the full IRT should be convened. For a “low” or “medium” severity incident, the responding member of the IRT has discretion to convene the IRT. If an incident is of “low” or “medium” severity and an IRT is deemed unnecessary, the incident will be noted, the reporting workforce member will be notified, and the incident will be considered closed.
5. The responding member of the IRT will authorize any actions that should be immediately taken (by the reporting employee or otherwise) to mitigate or remedy the situation.

*For an incident that is of “low” or “medium” severity and an IRT is deemed unnecessary the incident can be completed at this stage.*
Incident Response Team Initial Responsibilities

1. If the IRT needs to be convened, a meeting should be coordinated immediately:

2. At the first meeting, the IRT should:
   a. Review the incident report and assessment available in the OneTrust Privacy Management Software.
   b. Scope the incident
   c. Identify and agree upon objectives for the incident response
   d. Assign initial duties such as containment and evidence preservation.

3. Identifying and engaging groups and individuals with relevant expertise is critical.
   a. External security and forensic expertise should be contacted immediately following the first meeting of the IRT to assist in the triage.
   b. Counsel should be contacted immediately following the first meeting of the IRT. Counsel should be consulted regarding possible law enforcement involvement, and/or the need for forensic investigation.
   c. Insurance should be contacted immediately following the determination that insurance policies held by organization might provide insurance coverage for the incident or require their notification.
Remediating

The IRT, or its designees as decided upon in the initial IRT meeting, are responsible for taking the following steps in response to a significant security incident:

✅ Containment Strategy

1. When relevant, a containment strategy should be implemented that will limit the damage to organisation resources.
   a. Containment may involve technical controls, such as:
      i. Disk locks to make immutable
      ii. Enable deny all NSG rule in front of compromised host/subnet
      iii. Move system to isolated subnet, ensure deny all NSG follow or is mirrored
      iv. Run vulnerability scans against host; run or allow forensics to be completed (internal or 3rd party)
   b. Containment may involve non-technical, such as:
      i. Contacting an external party that has received confidential information in error.

✅ Collection of Evidence (ISO 27001 – Annex A 16.1.7)

1. Consideration should be given to preserving evidence during triage and scoping particularly if it becomes apparent that the incident involves criminal activity. Proper preservation of evidence requires establishment of chain of custody procedures. Any electronic evidence should be properly tracked in a documented and repeatable process. Preservation of evidence is also required for the purposes of insurance coverage, and failure to do so may limit or impact insurance recovery—consult with counsel for incident-specific guidance.
Forensic Analysis

1. Forensic analysis entails a technical examination of evidence, preservation of that evidence, preservation of the chain-of-custody of the evidence, documentation of observations, and analysis drawn from logical conclusions based on the evidence, absent opinion or conjecture.

2. Develop and record a hypothesis:
   a. How does the evidence support/contradict it?
   b. What did you do, what evidence did you find, and how did you test the hypothesis?
   c. What important interactions took place?

Retention of Evidence

1. Evidence records should be retained according to a set retention schedule (for example, for a minimum of one (1) year). Appropriate destruction of evidence records is permitted after that period if they are no longer needed by the organization.
Notifying

**Communication/Disclosure Strategy**

1. Proper handling of internal and external communications is critical in the initial phases of incident response.

2. Legal counsel should be consulted to determine whether the investigation will proceed under the direction of counsel and attorney-client privilege. If so, counsel may establish procedures for communication and documentation.

3. Review (and possibly deploy) prepared statements for all of the critical audiences that were prepared before the incident occurred in a joint effort of the Public Relations lead and the IRT.
   a. Ensure your Customer Support teams have a scripted response
   b. Ensure leadership has appropriate internal messaging
   c. If necessary, post messages to your public website or application providing customers with necessary information.

**Assessment of Incidents for Legal Reporting**

1. The IRT must perform an analysis to determine whether the information at risk is protected by state and/or federal laws and regulations requiring breach determination and notification.

2. Comprehensive information that maps out all applicable legal requirements is essential and OneTrust's Privacy Management Software can be used to automate this review to increase accuracy of the assessment and the speed of the response.

*If it is determined that notification is not required, the incident can be completed at this stage*
Notification Process

1. Communications Plan: identify who needs to be notified (internal / external), who is responsible; develop internal FAQs; press release draft; escalation guide for call center; formal notification to other agencies, vendors; media contact persons; press briefing. Identify the victims of data breach and cross-reference with other databases to compile the most recent contact addresses. Refer to legal and contractual requirements for notification timing requirements.

2. Develop a Call Center: Decide on using an internal vs external call center; toll-free telephone number; determine the staffing (numbers) and coverage hours and days of week; train staff to respond to incident calls (provide standard scripts); comfortable setting (head-sets, quiet area, computer); bi-lingual skills, etc.

3. Notification methods: Follow legal requirements as assessed in the OneTrust Privacy Management Software but in many cases, provide first class mail reporting to affected individuals, or email if specified as a preference. Determine whether the mail house is required to cleanse the list with National Change of Address Office. Notification by phone in “urgent cases”

4. Regulatory agencies: Determine which agencies (e.g., FTC), if any, require notification; provide each agency with their required information, in the format and manner (electronic, written, etc.) they require.

Notification Details:

1. Reports to external organisations, individuals or federal or state agencies include (when legal and necessary):
   a. a brief description of what happened;
   b. the date of the breach;
   c. the date of the discovery of the breach;
   d. a description of the types of information that were involved in the breach;
   e. the recommended steps external entities should take to protect themselves from potential harm resulting from the breach;
   f. a brief description of the steps the organisation is taking to:
      i. investigate the breach,
      ii. mitigate damages, and
      iii. protect against any further breaches;
   g. contact procedures to ask questions or learn additional information.
Complete

Learning from Information Security Incidents (ISO 27001 – Annex A 16.1.6)

Post incident actions should identify any areas where different technical, physical and/or administrative remediation measures would have improved results in this environment. Analyse whether those “upgrades” could and should be applied to other areas within the larger environment. If so, the Privacy/Security Lead must recommend how to apply these improvements.

ONLINE DEMO AND FREE TRIAL AT ONETRUST.COM

DISCLAIMER

No part of this document may be reproduced in any form without the written permission of the copyright owner.

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. OneTrust LLC shall have no liability for any error or damage of any kind resulting from the use of this document.

OneTrust products, content and materials are for informational purposes only and not for the purpose of providing legal advice. You should contact your attorney to obtain advice with respect to any particular issue. OneTrust materials do not guarantee compliance with applicable laws and regulations.

Copyright © 2018 OneTrust LLC. All rights reserved. Proprietary & Confidential.