IT Security Information Breach Notification Policy

Contents

Distribution List

☐	CEO	☐	COO
☐	CFO	☐	Country Managers
☐	Internal Only	☐	Internal and External
☐	All Staff	☐	Board Members

A. Introduction

An information technology (IT) security incident is an event involving an IT resource at *CompanyX* that has the potential of having an adverse effect on the confidentiality, integrity, or availability of that resource or connected resources. Resources include individual computers, servers, storage devices and media, and mobile devices, as well as the information, messages, files, and/or data stored on them. Prompt detection and appropriate handling of these security incidents is necessary to protect *CompanyX* information assets and to preserve the privacy and confidentiality of personal data.

The purpose of this *IT Security Information Breach Notification Policy* is to provide general guidance to *CompanyX* to enable quick and efficient recovery from security incidents; respond in a systematic manner to incidents and carry out the steps necessary to handle an incident; and minimize disruption to critical computing services or loss or theft of sensitive or mission critical information.

The sections below describe: 1) Who to notify upon discovery of an incident; 2) procedures for handling and recovering from an incident in a manner appropriate to the type of security incident; and 3) how to establish a reporting format and evidence retention procedure. This document provides an overview of the process. Detailed technical procedures can be found in *CompanyX* IT/ Global Office of Information Security (GOIS) internal documentation, including the Data Breach Investigation template.

This *IT Security Information Breach Notification Policy* also applies to Breaches concerning all *CompanyX* Covered Components and Support Components, and to all *CompanyX* Business Associates.

One of the most significant requirements is to notify individuals when there is a Breach of unsecured information. In addition, Business Associates and their subcontractors are directly liable for compliance and must provide proof of their efforts to prevent Breaches.

In the event of a Breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, GDPR Data (“GDPR Breach”), *CompanyX* is legally required to assess the risks to data subjects and may be required to notify data protection authorities and affected data subjects.

“GDPR Data” includes any personal information that is transmitted, stored, or otherwise processed by *CompanyX* relating to an identified or identifiable natural person that is subject to the European Union (EU) General Data Protection Regulation (“GDPR”). An identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, or an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. For further guidance as to which personal information is subject to the GDPR, please consult with *CompanyX* GDPR Data Protection Officer (the “DPO”).

In order to comply with the requirements of the GDPR, it is critical that all of the steps outlined in this Policy occur within seventy-two (72) hours of the first point at which an incident is discovered. In all cases, regardless of jurisdiction, the process must be completed as expeditiously as is reasonably feasible.

B. Overview of Workflow

When a security incident is detected or reported, key first steps are to (1) contain the incident, (2) initiate an investigation of its scope and origins, and (3) decide if it qualifies as a Breach.

If High Risk or GDPR Data is present on the compromised system, the Critical Incident Response (CIR) is followed.

C. Overview of Roles

1. Incident Handler: This role is filled by IT security staff from *CompanyX* and its IT Service Provider.
2. System Administrator: This role is filled by the technical staff responsible for deploying and maintaining the system at risk. Also referred to as a "first responder" in the context of this process.
3. System Owner: This role is filled by the staff member or management member who has responsibility for the business function performed by the system. The System Owner is not necessarily the person who paid for the system, but rather the person who has control over it.
4. Network Operations: This role is filled by the technical staff responsible for network infrastructure at the site housing the system at risk as undertaken by the *CompanyX* Service Provider.
5. PCI Compliance Manager: This role is filled by the person responsible for overseeing the *CompanyX* compliance program.
6. DPO: This role is filled by *CompanyX* GDPR Data Protection Officer, who may be assisted by designated personnel.

D. Identification

The identification phase of incident response has as its goal the discovery of potential security incidents and the assembly of an incident response team that can effectively contain and mitigate the incident:

1. **Identify** a potential incident. The incident handler may do so through monitoring of security sensors. System owners or system administrators may do so by observing suspicious system behaviours. Any member of *CompanyX* may identify (i.e., detect) a potential security incident though external complaint/notification, or other knowledge of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, High Risk Data or GDPR Data.
2. **Notify**: Employees of *CompanyX* that suspect an IT system or paper-based files have been subject to accidental or unlawful destruction, loss, or alteration, or unauthorized disclosure or access, must immediately report the situation to security@*CompanyX.com*. Once the incident handler is aware of a potential incident, s/he will alert local system administrators. If an incident is discovered by a member of the Covered Component or Support Component or by a Business Associate, the person should notify the GOIS. No one should interact with the system, unless approved by GOIS.
3. **Quarantine**: The incident handler will quarantine compromised hosts at the time of notification unless they are on the Quarantine Whitelist. If they are on the Quarantine Whitelist, the incident handler will promptly reach out to the system administrator or system owner to create a plan to contain the incident. Note that the incident handler may notify on suspicious behaviour when s/he is not confident of a compromise; in these cases, they do not quarantine the host immediately, but wait 24-48 hours and quarantine only if the registered contact is unresponsive.

E. Verification

This phase, and has the primary goal of confirming that the compromise is genuine and presents sufficient risk to engage the Data Incident Response (DIR process:

1. Classify: The DIR must be initiated if...
    1. The system owner or system administrator indicates that the system is a High Criticality System.
    2. or the system owner or system administrator asserts that the system contains High Risk Data.
    3. or someone of appropriate authority (for example, an IT Specialist) determines that the system poses a unique risk that warrants investigation.
2. Verify: The DIR process should be initiated only if...
    1. The incident handler verifies that the triggering alert is not a false positive. The incident handler will double-check the triggering alert and correlate it against other alerting systems when possible.
    2. and the type of data or system at risk is verified to be of an appropriate classification, as determined above. The system owner or system administrator should provide a detailed description of the data at risk, including approximate numbers of unique data elements at risk, and the number, location, and type of files it is stored in.

The order of the steps above can vary from incident to incident, but for the DIR process to be initiated the criticality of the asset must be confirmed, and it must be confirmed that the triggering event is not a false positive. In cases where the DIR process is not required, the incident handler can resolve the case as follows:

1. Obtain a written (email in the helpline ticketing system is acceptable) statement from the system owner or system administrator documenting that the system has no High-Risk Data or GDPR Data and is not a high-criticality asset.
2. Obtain a written statement from the system owner or system administrator that the system has been reinstalled or otherwise effectively remediated before quarantine is lifted.
3. Obtain a written statement that the access point has been disabled for incidents involving an unauthorized wireless access point.

F. Containment

The containment phase represents the beginning of the CIR workflow and has the following goals:

1. If the host cannot immediately be removed from the network, the incident handler will initiate a full-content network dump to monitor the attacker's activities and to determine whether interesting data is leaking during the investigation.
2. Eliminate attacker access: Whenever possible, this is done via the incident handler performing network quarantine at the time of detection and by the system administrator unplugging the network cable. In rare cases, the incident handler may request that network operations staff implement a port-block to eliminate attacker access. In cases where the impact of system downtime is very high, the incident handler will work with system administrators to determine the level of attacker privilege and eliminate their access safely.
3. The incident handler will collect data from system administrators in order to quickly assess the scope of the incident, including:
    1. Preliminary list of compromised systems
    2. Preliminary list of storage media that may contain evidence
    3. Preliminary attack timeline based on initially available evidence
4. Preserve forensic evidence:
    1. System administrators will capture first responder data if the system is turned on. The incident handler will provide instructions for capturing this data to the individual performing that task.
    2. The incident handler will capture images for all media that are suspected of containing evidence, including external hard drives and flash drives. System administrators will deliver the system to GOIS after the first responder data is captured; disk imaging and analysis will occur at GOIS. The system owner should expect to have it returned within five (5) business days.
    3. The incident handler will dump network flow data and other sensor data for the system.
    4. The incident handler will create an analysis plan to guide the next phase of the investigation.

This is the most time-sensitive and also the most contextually dependent phase of the investigation. The actions that need to be taken will depend on the uptime requirements of the compromised system, the suspected level of attacker privilege, the nature and quantity of data at risk, and the suspected profile of the attacker. The most important goals of this phase are to eliminate attacker access to the system(s) as quickly as possible and to preserve evidence for later analysis.

Additionally, this is the phase where the incident handler works most closely with system administrators and system owners. During this phase they are expected to take instruction from the incident handler and perform on-site activities such as attacker containment, gathering first response data, and delivering the system to GOIS in cases where host-based analysis is required.

G. Analysis

The analysis phase is where in-depth investigation of the available network-based and host-based evidence occurs. The primary goal of analysis is to establish whether there is reasonable belief that the attacker(s) successfully accessed High Risk Data or GDPR Data on the compromised system. Secondary goals are to generate an attack timeline and ascertain the attackers' actions. All analysis steps are primarily driven by the incident handler, who coordinates communications between other stakeholders, including system owners, system administrators, and relevant compliance officers. Questions that are relevant to making a determination about whether data was accessed without authorization include:

1. *CompanyX*

In the case of a potential GDPR Breach, this analysis will include the involvement of the *CompanyX* Data Protection Officer. The analysis will include an evaluation of the likelihood of risk to data subjects, including, for example, risks related to identity theft or fraud, financial loss, damage to reputation, and discrimination. The analysis should include whether the data has been encrypted, coded, or protected through other technological controls from use by an unauthorized person. The process and facts considered in reaching a determination as to the likely risks to data subjects must be documented.

Exceptions to the definition of a Breach are:

1. Any unintentional acquisition, access, or use of protected information by a team member or person acting under the authority of a Covered Entity or a Business Associate, if such acquisition, access, or use was made in good faith and within the course and scope of authority and does not result in further access, use, or disclosure.
2. Any inadvertent disclosure by a person who is otherwise authorized to access protected information to another person authorized to access protected information at the same Covered Entity or Business Associate in which the Covered Entity participates, and the information received as a result of such disclosure is not further accessed, used, or disclosed.
3. A disclosure of protected information where a Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

In the case of a potential breach of Information, GOIS will conduct a risk assessment to determine the probability that a “breach of the security of the system" has occurred, which is defined to mean an unauthorized access to or acquisition of, or access to or acquisition without valid authorization of, computerized data that compromises the security, confidentiality, or integrity of Private Information maintained by *CompanyX*. Good faith access to, or acquisition of, Private Information by an employee or agent of *CompanyX* for the purposes of *CompanyX* is not a breach of the security of the system, provided that the Private Information is not used or subject to unauthorized disclosure.

In determining whether information has been accessed, or is reasonably believed to have been accessed, by an unauthorized person or a person without valid authorization, GOIS may consider, among other factors, indications that the information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person.

In determining whether information has been acquired, or is reasonably believed to have

been acquired, by an unauthorized person or a person without valid authorization, GOIS may consider the following factors, among others:

1. indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or
2. indications that the information has been downloaded or copied; or
3. indications that the information was used by an unauthorized person, such as fraudulent accounts opened, or instances of identity theft reported.

If, during analysis, it appears probable that High Risk Data (including Private Information) or GDPR Data has been exposed, the incident handler should consult with the COO team to determine the appropriate Officials to inform regarding the situation and also determine the extent of the *CompanyX* notification and reporting obligations.

At the conclusion of the analysis, but before the final report is written, a peer review should be requested of the other GOIS technical staff. Then, the write-up of the notes should be completed, including conclusions, and processed source materials (e.g., grep-results, file-timelines, and filtered flow-records) should be archived. The peer review may result in some issues that must be addressed and some issues that may optionally be addressed. All recommendations should be resolved or acknowledged and deferred. The incident handler's role is to determine, from a technical perspective, whether there is a reasonable belief that High Risk Data or GDPR Data, was available to unauthorized persons. The determination of whether the circumstances warrant a Breach notification will be made jointly by the COO team and the IT Service Provider

H. Recovery

The primary goal of the recovery phase is to restore the compromised host to its normal business function in a safe manner.

1. The system administrators will remediate the immediate compromise and restore the host to normal function. This is most often performed by reinstalling the compromised host; although if the investigation confirms that the attacker did not have root/administrator access other remediation plans may be effective.
2. The system administrators will make short-term system, application, and business process changes to prevent further compromise and reduce operating risk.

I. Internal Reporting

The final report serves two (2) main purposes. First, a recommendation is made as to whether the incident handler and the responsible officials feel there is a reasonable belief that High Risk or GDPR Data was subject to accidental or unlawful destruction, loss, or alteration, or unauthorized disclosure or access, and the degree of probability of risks to data subjects or that the security or privacy has been compromised. The report must be made in sufficient time to allow notification, if appropriate, within any legally mandated time period. As noted, under the EU GDPR, notification to authorities must occur, wherever feasible, within seventy-two (72) hours of discovery of a GDPR Breach.

Second, a series of mid-term and long-term recommendations are made to the owners of the compromised system/files, including responsible management, suggesting improvements in technology or business process that could reduce operating risk in the future.

1. The incident handler will draft the final report after the investigation is complete. Preliminary reports should be avoided whenever possible since working conclusions can change substantially through the course of an investigation.
2. After the draft report is completed, signoff on the content of the report should be obtained from GOIS management. Technical personnel can offer comments now as well, but typically technical issues should be resolved by this stage. Again, a list of issues will be raised which should be resolved or acknowledged/deferred until GOIS management accepts the report.
3. For critical incidents involving payment card data, the Compliance Manager will receive a copy of the report and appropriate entities will be notified in the event that cardholder data is accessed without authorization. The Compliance Manager will be responsible for all communications and will be responsible for coordinating the activities with respect to the incident.
4. For incidents involving GDPR Data, the report will address each accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, GDPR Data.
5. The incident handler will schedule a meeting to deliver the final report to the system administrator, the system owner, as well as to responsible officials. Although the correct management contact will vary on a case-by-case basis, it should typically be Director-level or above. Do not distribute electronic copies of the report via email.
6. The incident handler will ensure that the final report includes the details of the investigation and mid-term and long-term recommendations to improve the security posture of the organization and limit the risk of a similar incident occurring in the future.

J. Data Retention

1. The incident handler will archive the final report in case it is needed for reference in the future; reports must be retained for six (6) years.
2. Incident notes should be retained for six (6) months from the date that the report is issued. This includes the confluence investigation page, processed investigation materials like grepped file-timelines and filtered network-flows, etc.
3. Raw incident data should be retained for thirty (30) days from the date that the report is issued. This includes disk-images, unfiltered Net activity, raw file-timelines, and other data that was collected but deemed not relevant to the investigation.
4. Request Tracker (RT) tickets from the ticketing system related to the investigation should be retained for three (3) years.

APPENDIX A: Breach of GDPR Data

1. Within twenty-four (24) hours of the discovery of a GDPR Breach, the DPO will make a determination as to whether reporting to supervisory authorities and/or data subjects is required by law or is otherwise prudent. A determination from the DPO that notification is required and the authorization from an authorized member of management will initiate the external notification procedure. Notification to EU data protection authorities is required unless a determination is made that the Breach is unlikely to result in a risk to data subjects. If the Breach is likely to result in a *High Risk* to data subjects, notification to data subjects is also required.

2. The DPO will determine the appropriate authorities to notify. Notification to authorities must: (i) describe the nature of the Breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Information records concerned; (ii) communicate the name and contact details of the DPO or other contact point where more information can be obtained; (iii) describe the likely consequences of the Breach; and (iv) describe the measures taken or proposed to be taken by *CompanyX* to address the Breach, including, where appropriate, measures to mitigate its possible adverse effects.

3. External reporting to the EU GDPR supervisory authorities must be conducted within seventy-two (72) hours of discovery of the security incident, wherever feasible. If any delay in reporting is necessary, the reasons for this delay must be documented. In all cases, external reporting must be conducted within thirty (30) days.

4. The business process owner of the compromised system/files will compile the list of the specific individuals whose GDPR Data is reasonably believed to have been accessed and/or acquired by an unauthorized person. When identification of specific individuals cannot be made, all individuals who are likely to have been affected, such as all whose GDPR Data is stored in the files involved, should be notified. The process for determining inclusion in the notification group must be documented.

5. The DPO, after consulting with the Office of General Counsel, will determine the plan for notifying individuals affected by the Breach consistent with the following guidelines:

- The method of notification –
    - In general, notices should be sent by postal mail or, preferably, email. *CompanyX* standard Breach notice will consist of an email message featuring the official CompanyX logo, addressed to the individual at the last recorded email address registered with *CompanyX*. Any notices returned as undeliverable should be re-sent via another channel, such as by first class mail, if alternate contact information is available.
    - In the case of a severe, widespread Breach of security, as determined by the DPO, (a) a "Notice of Breach" must be conspicuously posted on *CompanyX* website; and (b) major media outlets, including television, radio, and print must be notified.

- The content of the notice –
    - The notice should include a description of the incident in general terms.
    - The notice should include a description of the type of GDPR Data that was the subject of the Breach.

    - The notice should include a description of the general acts of *CompanyX* to protect the information from further unauthorized access and/or acquisition.
    - The notice should include a telephone number that the individual may call for further information and assistance; and
    - The notice should include advice that directs the individual to remain vigilant by reviewing account statements and monitoring free credit reports, where applicable to the nature of the Breach.

- The timing of notification –
    - Affected individuals must be notified in the most expedient time possible, and without unreasonable delay, consistent with any measures necessary to determine the scope of the Breach and to restore the reasonable integrity of the data system.
    - Delay is permitted when a law enforcement agency has determined that notification will impede a criminal investigation. In such a case, notification must occur as soon as the law enforcement agency determines that notification will no longer compromise the investigation. The factors considered when determining the timing of notification must be documented.