

**BLUEIT**

**NOTIFICATION**

 **PROCEDURE**

CONTENTS

[Process flow 3](#_Toc195187688)

[Process 3](#_Toc195187689)

[Purpose 3](#_Toc195187690)

[Scope 3](#_Toc195187691)

[Procedure 4](#_Toc195187692)

[Why report an incident? 4](#_Toc195187693)

[Type of notification 5](#_Toc195187694)

[To whom should you make a report? 7](#_Toc195187695)

[How should you report an incident? 8](#_Toc195187696)

[Version history 9](#_Toc195187697)

# Process flow

F-ISM-002-FLOW DATA BREACH

# Process

## Purpose

The objective of an ISO 27001 incident notification procedure is to ensure a consistent and effective approach to managing information security incidents.

This includes quickly detecting, reporting, responding to, and resolving incidents to minimize the impact on the confidentiality, integrity, and availability of information.

Key objectives include:

* **Protection of sensitive information**: Prevent confidential data from falling into the wrong hands.
* **Business continuity**: Ensuring that business processes are disrupted as little as possible

by incidents.

* **Compliance with laws and regulations**: Comply with legal and contractual requirements related to information security.
* **Improving security measures**: Learning from incidents to reduce future security risks.

## Scope

The scope of an information security incident reporting procedure under ISO 27001 includes all activities and processes required to identify, report, manage and resolve information security incidents.

This includes:

* **Incident identification**: Detecting potential information security incidents, such as data breaches, unauthorized access, malware attacks, and so on.
* **Incident Notification**: Recording and reporting incidents to the appropriate individuals or departments within the organization.
* **Assessment and classification**: Evaluating the severity and impact of the incident to determine appropriate action.
* **Response and recovery**: Taking corrective actions to mitigate the impact of the incident and restore normal operation.
* **Documentation and reporting**: Maintaining detailed records of the incident and actions taken for future reference and regulatory compliance.
* **Evaluation and improvement**: Analyzing incidents to learn lessons and improve security measures to prevent recurrence.

This scope ensures that the organization is prepared for different types of information security incidents and that there is a structured approach to managing them effectively.

## Procedure

The procedure includes the following topics:

* Why report an incident?
* Type of notification?
* To whom should you make a report?
* How should you report an incident?

### Why report an incident?

* **ISO 27001**: 'Continuous improvement' is central to every ISO standard. This is only possible if the organization is aware of what is happening, both internally and externally (customers, suppliers, prospects, market trends, legislation, media, etc.).
* **GDPR legislation**:
	+ Every data breach MUST be registered. If serious, it must also be reported to the Data Protection Authority, sometimes also to the data subjects
	+ Each data subject has a number of rights that he or she can exercise
	+ A transfer of personal data outside the EEA (= to third countries) is only allowed with an adequate level of protection.

### Type of notification

* **Incidents**: is an event in which the security of information, hardware, software, a process or an organization may have been compromised.

This could be a security breach, a virus infection, a power outage, or a lost document. Incidents do not always have to be personal data and therefore do not always have to be reported to the Dutch Data Protection Authority (AP).

Here are some examples of security incidents that are not data breaches:

* + **Loss of an encrypted laptop**: If a laptop is lost, but the data on it is fully encrypted and inaccessible without proper authorization, it is a security incident but not a data breach.
	+ **Network outage**: A temporary network outage that renders systems unavailable, but does not expose personal data.
	+ **Unauthorized access attempt**: An attempt at unauthorized access to a system that is detected and blocked before accessing personal data.
	+ **Error in software**: A bug in the software that affects functionality but does not expose personal data.
	+ …

These incidents still require attention and possible measures, but they do not fall under the obligation to report data breaches because no personal data has been exposed.

* **Data breach**: everything related to ***information security*** and ***personal data***.

When do we speak of a data breach?

* + In case of **loss or theft of data or equipment containing data** (laptop, mobile phone,...)
	+ In the event of **unauthorised modification or disclosure of processed data**
	+ In **hacking**
	+ In case of **human error**, e.g. Sending an email incorrectly containing:
		- Passwords
		- Financial data
		- Plans (e.g. implementation plan)
		- Quotations, contracts,...
	+ In the **event of significant data unavailability**,
	+ ...

***A data breach is very broad***: complaint, incident, improvement proposal, tendency, ... both internally and externally, e.g. Also comments from customers, prospects.

**Important**: only describe the errors. Who made the mistake is not important.
E.g.: 'prints regularly remain on the printer'. Then an email is sent out with a reminder to pick up the prints directly at the printer.

* **Rights of data subjects**: Each data subject or data subject has the right to access, correct, erase, restrict processing, transfer to another controller, object to the processing and refuse automatic decision-making, including profiling (BlueIT does not do automatic decision-making or profiling).

In addition, any data subject can also file a complaint with the Data Protection Authority. The data subject can exercise a right by asking BlueIT (e.g. in the case of a misspelled name: 'please correct my name in all your files'). The answer (e.g. the correction) must be done within a period determined by the GDPR legislation, otherwise a (serious) administrative fine can be imposed.

* + - If you receive an e-mail, message, letter, etc. in which 1 or more rights are exercised by a data subject, this must be **immediately** passed on to the ISMS manager by mail to intel@blueit.be , so that he can respond within the deadline.
* **Transfer of personal data outside the EEA** (EEA = all countries of the European Union and Iceland, Norway and Liechtenstein).

All transfers of personal data that do not take place within this EEA must be reported to the ISMS Manager before the transfer takes place, so that he can verify the necessary protective measures.

Only when that check has been carried out and the appropriate level of protection is guaranteed, the data may be forwarded. This is an important obligation within the GDPR legislation.

### To whom should you make a report?

* To the **ISMS-Manager of BlueIT**.
	+ **Data breach** 🡪 **Immediately**
		- Suspicion that password is known by third parties
		- Loss of badge
		- Possible or actual breaches of the acceptable use of company resources (= the information itself and the company resources containing it)
		- Suspicion of misuse of material left unattended
		- Loss of company resources: laptop, mobile phone (even if yours), external drive, etc
		- Wrong mail with important information
	+ **Other** 🡪 as soon as possible
		- In the event of a suspicion or determination that a user has access to files or networks to which he is not authorised = more access by the user than is necessary for the proper performance of his tasks
		- Unavailability of data.
* **Why report immediately?** 🡪 Depending on the severity of the data breach, this should:
	+ Be reported to the Data Protection Authority **within 72 hours** of becoming aware
	+ In some cases also without delay to the data subjects
		- BlueIT must be able to determine the severity within that time!
* **Exercise of the right by the person concerned**: **immediately** report to the ISMS manager.
* **Transfer of personal data outside the EEA**: **before** such transfer takes place, to the ISMS Manager.

### How should you report an incident?

* To the ISMS Manager by mail to intel@blueit.be
* You must provide the following information by e-mail:
	+ **Incident or data breach**
		- **Date** incl. **time**
		- **Type of notification**: e.g. complaint, incident, improvement proposal,…
		- **Short information:** Which data & which people are involved
			* Description of data subjects and type of personal data
			* Estimate of the number of data subjects and the number of personal data
	+ **Rights of the data subject**: integral forwarding of the mail / letter / message to intel@blueit.be
	+ **Transfer of personal data outside the EEA**: physical address of the recipient (= to whom the data will be sent)

# Version history

|  |
| --- |
| **TEMPLATE REFERENCE 003** |
| **VERSION** | **MODIFIED BY** | **DATE** | **SUMMARY** | **VERIFIED BY** | **DATE** |
| **001** | Kimberly Huysman | 13-03-’25 | NEW DOCUMENT  | Thomas Mariën | 13-03-‘25 |
| **002** | Kimberly Huysman | 10-04-‘25 | CHANGES | Thomas Mariën | 10-04-‘25 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |