|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |
| --- |
| Information Security Incident Management Policy  |
| Organisation: [Organisation] |
| Information classification: [Category] |

Document Control

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Updated by | Date | Description of changes |
| 1.0 | [Name, Surname] | [Publish Date] |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Reviewed by | Reviewer Role | Approved by | Date | To be reviewed by |
| [Name, Surname] | [Role] | [Name, Surname] | [Publish Date] | [Next Review Date] |

|  |  |  |
| --- | --- | --- |
| Document owner | An electronic copy of this document is stored at | A physical copy of this document is stored at |
| [Name, Surname] | [Location] | [Location] |

 |

Table of contents

[1. Context 3](#_Toc126850226)

[1.1. Purpose of this document 3](#_Toc126850227)

[1.2. Scope of this document 3](#_Toc126850228)

[1.3. Roles and Responsibilities 3](#_Toc126850229)

[1.4. Definitions 4](#_Toc126850230)

[1.5. Policy Enforcement 4](#_Toc126850231)

[2. Policy statements 5](#_Toc126850232)

[2.1. Responsibilities and procedures 5](#_Toc126850233)

[2.2. Preparing for information security incidents 5](#_Toc126850234)

[2.3. Detecting information security incidents 5](#_Toc126850235)

[2.4. Reporting of information security incidents 5](#_Toc126850236)

[2.5. Response to information security incidents 6](#_Toc126850237)

[2.6. Collection of evidence 6](#_Toc126850238)

[2.7. Learning from information security incidents 6](#_Toc126850239)

[Annex: Explanatory Notes 7](#_Toc126850240)

[Policy specific 7](#_Toc126850241)

[Further reference documentation 11](#_Toc126850242)

# Context

Information security incidents impose a significant threat to because of the impact they can have on our activities (e.g., capabilities, reputation) and organisational functions (e.g., personnel, infrastructure, software). The purpose of incident management is to reinstate normal service operations as fast as possible and mitigate the negative impact on activities.

The goals of incident management are to:

* Organize for the collection and detection of information security events and incidents;
* Confirm whether an incident occurred;
* Provide a defined incident notification process;
* Promote the collection and documentation of accurate information;
* Establish controls for proper retrieval and handling of evidence;
* Contain the incident and stop any unwanted activity quickly and efficiently;
* Minimize disruption to operations;
* Provide accurate reports and useful recommendations to management; and
* Prevent and/or mitigate future incidents from occurring.

## Purpose of this document

The purpose of this document is to define the approach that [Organisation] shall follow to prepare, detect and respond to information security incidents. The aim is to ensure that [Organisation] properly prepares, identifies, contains, investigates, remedies, reports and responds to information security incidents.

## Scope of this document

This policy is applicable to information security incidents related to information, Information Technology (IT) systems, infrastructure, and people. It is also applicable to the full information security incident management lifecycle, including reporting of, assessing of, responding to, communicating on, and learning from confirmed and potential information security incidents. This policy applies to all [Organisation] information and functions, with a target audience of employees and contractors involved in information security incident handling.

## Roles and Responsibilities

The table below describes the [Organisation] roles and their description. Each business and security operations role can be updated with roles or positions of the responsible person as applicable.

| Role | Description |
| --- | --- |
| [Organisation Responsible] | The person belonging to the management of [Organisation] responsible to implement this policy internally. |
| [IT Responsible] | The employee of [Organisation] responsible to act with accordance to this policy in case of an information security. |
| [Organisation IT Helpdesk] | The employee or team of [Organisation] responsible to be the first point of contact of employees and contractors of [Organisation] in case of an information security incident. |
| Employees and contractors | All personnel delivering a professional service under a legal agreement for [Organisation]. |
| [Department Representatives] | Any individual responsible for a specific department of [Organisation] activities. |
| Third Parties | Any non-employee of [Organisation] who is contractually bound to provide some form of service to [Organisation]. |
| External Parties | Any external organisation, association, or legal Organisation that the [Organisation] can communicate with when relevant for the management of information security incident. |

## Definitions

The following table defines all the acronyms and terms used in this document:

| Term  | Definition |
| --- | --- |
| Information security incident | A single or a series of unwanted or unexpected cyber security events that are likely to compromise organisational activities. |
| Root Cause Analysis (RCA) | Approach for investigating the underlying cause of a an incident so that appropriate measures can be taken to prevent the incident from reoccurring. |
| Mitigating measures | Refers to a control put in place to protect IT systems, data and applications from cyber threats. Measures can involve prevention, detection, and response to such attacks. |
| Vulnerability | A flaw or weakness in a computer system, its security procedures, internal controls, or design and implementation, which could be exploited to violate the system security policy. |

At its first appearance in the document, a term from this table is printed in *italic.*

## Policy Enforcement

1. The policy statements containing the terms “*shall*” and “*shall not*” indicate a requirement, while the terms “*should*” and “*should not*” indicate a recommendation.
2. Without a formally approved exception, non-compliance with the policy statements can be subject to disciplinary actions in accordance with [Organisation] Human Resources policies and processes.
3. All parts of the document indicated inside [ ] and highlighted in light blue (#60BCCF) must be tailored by the role in charge of developing this policy in accordance with [Organisation] structure, context, and needs.

# Policy statements

## Responsibilities and procedures

1. Information security incident management procedures shall be documented, implemented and maintained.
2. Information security incident management procedures shall cover at minimum:
* An incident response plan detailing how to analyse, contain, eradicate, recover and learn from *information security incidents*;
* Incident handling and reporting procedures including reporting evidence to authorities and information security incidents playbooks;
* Internal and external communication guidelines, including crisis communication principles;
* Training guidelines, including for simulation exercises.
1. Roles and Responsibilities shall be clearly defined for each procedure.
2. Information security incident related information shall be treated as confidential.
3. [IT Responsible] shall inform all [Organisation] employees and contractors of the action to be taken in case of an information security incident.
4. [Department Representatives] shall provide contact information for their primary and secondary representatives, and immediately notify of any changes to that information.
5. The procedure for reporting information security incidents should be easy, clear, accessible and readily available for the intended audience (including employees, contractors, customers and public).

## Preparing for information security incidents

1. Escalation of incidents shall be straight forward with a direct communication line between [IT Responsible] and [Organisation Responsible] in case of significant incidents.
2. Criteria for when an information security incident becomes a crisis should be defined (e.g., on the basis of the impact on business services or the period of unavailability of IT services).
3. The roles and responsibilities of External Parties or suppliers in case of information security incidents should be clarified, especially regarding support.
4. Use cases for most common threats and *vulnerabilities* should be defined to monitor for specific information security events.
5. Simulated information security incidents should be tested periodically, at least once a year, to facilitate effective response by [Organisation] personnel and [Organisation IT Helpdesk]. The lessons learned shall be documented and used to further improve the effectiveness of incident response.
6. Information security incident playbooks should be available to [Organisation] personnel and [Organisation IT Helpdesk] to mitigate common information security incidents (e.g. ransomware).

## Detecting information security incidents

1. Logging of systems alerts, vulnerabilities, user actions shall be used to track information security incidents.
2. Monitoring of systems alerts, vulnerabilities and logs should be used to actively detect information security incidents.

## Reporting of information security incidents

1. [Organisation] employees and contractors shall report immediately any suspected or confirmed information security incident to [Organisation IT helpdesk] at [Email address ; Phone number ; Ticketing system URL].
2. [IT Responsible] shall inform all employees and contractors of what is considered as a (potential) security incident, their responsibility to report information security incidents, as well as how and where to report them.
3. Reports to [Organisation Responsible] should include a summary of the information security incidents, the root cause, business and IT functions affected as well as proposed and remediation actions taken.
4. Information security incidents’ impact shall be categorized with a scale [Critical ; Important ; Medium ; Low] to facilitate proper escalation. In case the information security incident is part of a personal data breach, this should be indicated in the reporting.
5. Incident’s status should be tracked and updated at least for significant information security incidents with categories [Pending ; Confirmed ; Resolved] throughout their life cycle.
6. [Organisation IT helpdesk] should provide feedback on individual(s) who reported the information security incident when the information security incident’s status is [Confirmed] and [Resolved].

##  Response to information security incidents

1. All confirmed information security incidents shall be responded to in accordance with the incident response plan that details how to analyse, contain, eradicate, recover and learn from incidents.
2. [Critical] information security incidents shall be communicated to [Organisation Responsible] and [IT Responsible].
3. Communication of information security incidents to external parties shall be done by authorized individuals only.
4. Reporting of information security incidents to relevant external parties [Data Protection Authority, Police, Sectoral Federation] shall be done as required by law or regulations.

## Collection of evidence

1. Evidence of information security incident which may lead to legal action shall be collected, retained and presented to satisfy the requirements for admissibility and weight of the evidence in the relevant jurisdiction(s).
2. The protection of collected evidence shall comply with access management procedures and all applicable legal requirements. An appropriate protection should consist of encrypting, safe storing and access restrictions to the evidence that were collected during information security incidents.

## Learning from information security incidents

1. Confirmed information security incidents shall be investigated to understand the root cause (at least for recurring and/or significant information security incidents).
2. Significant information security incident reports shall be reported periodically to [Organisation Responsible] and shall include type, volume, impact and lessons learned.
3. All [Organisation] employees and contractors shall be trained on the management of information security incidents. to reduce the likelihood or impact of recurring or high impact information security incidents.
4. A monitoring of Information systems shall be implemented to reduce the likelihood or impact of recurring or significant impact information security incidents.
5. *Root Cause Analysis* should lead to the identification of *mitigation measures*.

# **Annex: Explanatory Notes**

## Policy specific

The information security incident management policy supports organisations in outlining the required activities upon handling different types of incidents. It provides the structure and procedural tools for them to respond, report and mitigate the information security incident before they have an impact on the organisation’s most important assets from a business and operational point of view, as well as to prevent legal consequences from occurring.

The information security incident management policy is usually complemented by an incident response procedure or playbook which acts as a descriptive action plan to respond to the threats in the organisation (cfr. [Incident Response Procedure]).

### Roles and Responsibilities

To support on the implementation of this policy and implement the roles identified in section 1.3. Roles and Responsibilities, please refer to the below overview of suggested incident response management tasks and main roles. Based on this, each organisation can assign the type of responsibility level as per the legend below. Additional roles can be assigned if relevant for the tasks listed in the table below.

|  |  |
| --- | --- |
| R | Responsible |
| A | Accountable |
| C | Consulted |
| I | Informed |

Additional roles can be assigned in line with the listed responsibilities. The first task was assigned as an example.

| Role Task  | [Organisation Responsible] | [IT Responsible] | Organisation IT Helpdesk | Employees and contractors | Department Representatives | [Other Role] |
| --- | --- | --- | --- | --- | --- | --- |
| Maintenance of the information security incident management procedures | **[A]** | **[R]** | **[C]** |  |  |  |
| Informing employees and contractors of required actions following and information security incident | **[A]** | **[R]** |  |  | **[I]** |  |
| Provision of relevant contact information to assigned primary and secondary representatives | **[A]** | **[R]** |  |  |  |  |
| Management of incident escalation requests | **[A]** | **[R]** | **[C]** |  |  |  |
| Ensuring information security incident periodical simulations and testing | **[A]** | **[R]** | **[I]** |  |  |  |
| Internal reporting of any suspected or confirmed information security incidents  | **[A]** | **[R]** | **[C]** |  | **[I]** |  |
| Informing employees and contractors of expected actions for reporting information security incidents | **[A]** | **[R]** | **[I]** |  | **[I]** |  |
| Handling, impact classification, tracking and updating of the information security incident | **[A]** | **[R]** | **[C]** |  |  |  |
| Provision of feedback to individuals who reported the information security incidents | **[A]** | **[R]** |  |  | **[I]** |  |
| Communication of relevant information security incidents to external parties | **[A]** | **[R]** |  |  | **[I]** |  |

### Ticket status

The table below complements section [2.4. Reporting of Information Security Incidents](#_Reporting_of_information_1) by indicating possible statuses of the incident response tickets:

|  |  |
| --- | --- |
| Status | Description |
| Pending  | A pending status request means that the system has received the report request. |
| Confirmed | The report request has been accepted and its being under review while working on the reported incident. |
| Resolved | The reported incident received by the request report has been successfully resolved. |

### Organisational functions

The table below complements section [2.4. Reporting of Information Security Incidents](#_Reporting_of_information_1) by indicating examples of organisational functions:

|  |  |
| --- | --- |
| Type | Description |
| Infrastructure | Function including the basic physical and organisational structures and facilities needed for the operation of [Organisation]. |
| Personnel | Function including all persons employed by [Organisation]. |
| Software | Function including programs and other operating information systems used by [Organisation] to achieve its functionality. |

### Information security incident classification levels

The table below complements section [2.4. Reporting of Information Security Incidents](#_Reporting_of_information_1) by indicating examples of incident classification levels:

|  |  |
| --- | --- |
| Level | Description |
| Critical | Critical category information security incidents affect the entire [Organisation] compromising the functionality of the whole corporation. |
| Important | Important category information security incidents affect multiple [Organisation] functions, compromising the smooth functionality of the corporation. |
| Medium | Medium category information security incidents affect small functions of [Organisation] with medium impact on the organisation processes. |
| Low | Low category information security incidents have small impact on low interest functions of [Organisation] without compromising the functionality of the corporation. |

### Information security incidents impact reduction measures

The table below showcases examples of the reduction measures mentioned in section [2.7 Learning from Information Security Incidents](#_Learning_from_information) that can be implemented to reduce the information security incidents impact:

|  |  |
| --- | --- |
| Security Measure | Description |
| Security Awareness Training | Ensure that all employees and contractor of the organisation knows enough about security to understand the need for it and to be vigilant in their day-to-day work about security dangers. Plan regular security trainings for all employees and contractors. |
| Audit Events | Ensure that activity on the system leaves a record that allows reliable after the information security incident investigations of information security incidents. Protect the records from unauthorized access and periodically review them. |
| Cryptographic Protection | Provide security properties by transforming information in mathematical formulas, employ the appropriate cryptographic formulas to protect all organisation information classified as requiring protection. |
| Information Sharing | Support authorized employees and contractors in taking secure decisions to share information with partners. Enable employees and contractors to determine if an intended recipient of information is authorized to access the information. Enable employees and contractors in making information sharing decisions through automated mechanisms or manual processes. |
| Security Assessment | Periodically assesses the security controls of the system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome and report the assessment result to the predefined individuals or roles in the organisation. |

## Further reference documentation

The table below showcases further documentation that can guide in the implementation of the policy:

|  |  |
| --- | --- |
| Title | Link to documentation (if available) |
| Information classification | <https://cert.be/en/traffic-light-protocol-tlp>  |
| Cyber Centre for Belgium Cyber Security Incident Management Guide | <https://ccb.belgium.be/en/document/cyber-security-incident-management-guide>  |
| Incident Reporting | <https://www.safeonweb.be/en/useful-links>  |
| NIST Cyber Security Framework:ID.GV GovernanceDE.DP Detection ProcessesRS.AN AnalysisRS.CO CommunicationsRS.RP Response PlanningRC.IM Improvements | https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf |
| [Indicate [Organisation] related documents and procedures] |  |