A logo of a yin yang

AI-generated content may be incorrect.

*Generic Company*

**Generic process manual for**

Security incidents  
Data breaches  
Major outages  
  
The sky is the limit really… ***version 1.0***

**Document information**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Version** | **Date** | **Description** |
| Generic major incident process manual | 1.0 | 02.09.2024 | A detailed process description on how to handle major incidents. |

**Opdateringslog**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Version** | **Change** | **Date** | **Page** |
| First Name, Last name  Email address | 0.8 | First draft | 02.07.2024 | All |
| First Name, Last name  Email address | 0.9 | Typo correction | 02.08.2024 | 4,5 |
| First Name, Last name  Email address | 1.0 | Changed company logo.  First release version | 02.09.2024 | 1 |

**Document Owner**

**First name, last name, department <email address>**

**Target group**

The target group for this document is.

* **Team A**
* **Team B**
* **Team C**

**Document review requirements**

This document must be reviewed every year.

**Purpose**

The purpose of the process description is to provide an overview of activities related to handling major incidents at Company.

Additionally, the document contains information and role descriptions for the core multidisciplinary expert group whose function it is to ensure quick and effective handling of major incidents.

By having a defined expert group, knowledge and experience are anchored, which is essential to ensure proper handling of incidents across the organization.

The team is responsible for managing the incident from discovery to mitigation.

The process manual is kept in English to facilitate clear and consistent communication among diverse stakeholders. However, the development of localized documentation is encouraged to enhance accessibility and understanding.

Illustrated below, are the different phases the incident must go through from discovery to resolution;

**Focus Points:** Stop or get the incident under control.

Identify and assign the ticket to the relevant incident manager.

Invite to the initial meeting

**Focus Points:**

Start incident log

Create an overview of the situation

Assess if communication (internal/external) is required

Assess if escalation is required

Identify stakeholders from the business

Create an activity plan with responsible parties

**Focus Points:**

Share knowledge and learn!

**Focus Points:**

Communicate closure to relevant stakeholders

Document all learning points

**Focus Points:**

Invite to follow-up meetings

Involve stakeholders from the business *(Leadership, Product Owners, etc.)*

**Focus Points:**

Resolve the incident

Restore normal operations

Prepare reporting to the relevant authorities if required

**Incident team**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **DPO/Legal** | **IT Security** | **IT Operations** | **Communication** | **Product Owner** |
| **Primary**  PersonA  <email address>  **Secondary**  PersonB  <email address> | **Primary**  PersonA  <email address>  **Secondary**  PersonB  <email address> | **Primary**  PersonA  <email address>  **Secondary**  PersonB  <email address> | **Primary**  PersonA  <email address>  **Secondary**  PersonB  <email address> | Ad-hoc basis  Product owners can be found in system X where all services are documented. |
| **Role**  Advisor regarding GDPR and privacy legislation, including how requirements for reporting and notifications are performed.  Secondary log keeper | **Role**  Advisor regarding IT security, policies, and rules.  Primary log keeper | **Role**  Operational lead and incident manager on all incidents involving IT infrastructure.  Secondary log keeper | **Role**  Responsible for internal and external communications.  Responsible for facilitating meetings.  Primary log keeper | **Role**  Owns the system on which the incident has occurred.  Responsible for documentation, follow-up tasks and learning. |

1. **Incident reported**

Any employee in the core team who becomes aware of an incident covered by the business process must ensure as soon as possible that the parties responsible are working to "stop the accident".

Ensure that a case is created in the ticket system.

Call for an initial meeting.

1. **Initial Meeting**

At the initial meeting, the focus is on creating an overview and agreeing on who should be involved.

The incident log is started by the log responsible.

An overview of tasks is started by the log responsible

The following must at a minimum be discussed and recorded in the incident log:

* What has happened and what is the status?
* Is any urgent action needed to stop the incident?
* Do we know where the incident occurred and why?
* Do we know when the incident occurred?
* Has there been a data breach?
* What is the extent of the incident, e.g., how many are affected?
* Does the incident affect our operations to such an extent that overall emergency management needs to be activated?
* Is there a need for communication (e.g., intranet or talking points/FAQ for customer front), external communication)
* Is there a need to involve external experts?

1. **Work the incident**

With IT Operations as lead, all members of the team ensure continuous updates of.

* **Log** (IT operations are the primary log keeper, everyone gives input)
* **Root cause analysis** (IT Operations)
* **Legal assessment** (DPO/Legal)
* **Task activity overview** (everyone)

1. **Follow-up meetings**

The communications responsible facilitate meetings as needed. The frequency and agendas of the meetings can vary based on the nature of tasks, blockers or stakeholder management.

1. **Follow-up meetings**

During the final meeting, the following checks are performed:

* All tasks on the activity list are completed.
* Recommendations on how to prevent similar incidents in the future and any follow-up controls are handed over to relevant stakeholders.
* Further work on mitigating measures and controls is documented in system X and assigned an owner.
* Relevant risk assessments of systems, processes, and/or vendors are updated.

1. **Incident closure**

* When all relevant information has been gathered and normal operations have been resumed, the incident can be closed.
* Log is updated and saved in system X
* Lessons learned from the incident are shared with relevant parts of the organization via relevant forums and communication channels.

Appendix

Incident #1337

Event log

Created by:   
First name, Last name, Email address.

**Summary**

*This is where you type the executive summary with relevant information in a not so detailed matter. Make it understandable for everyone including your mother.*

**Timeline**

|  |
| --- |
| **Initial meeting 01.08.2024 @ 10:45**  *This is where you keep a log of meetings, agreements, actions etc. This is very handy when you need to do post-mortems or retrospectives. This log can be very, very long – and that’s fine.*  *Keep a line for every meeting, action, new information etc.* |
|  |
|  |
|  |
|  |

**Root Cause Analysis**

*This is where you either write or link to the detailed root cause analysis that includes all the technical information.*

**Observations and learning**

*This is where you document all the things you learned, and how you are going to learn going forward. Ensure that all observations and learnings is assigned to a responsible person, and that regular status updates are performed.*