Emergency Plan for   
**<Insert Customer Name>**

# Emergency Action

## Actions

## First step during emergency

|  |  |  |
| --- | --- | --- |
| Step | Description | Responsible |
| 1 | **Decide whether emergency plan must be activated.**  All who is decision responsible, is authorized to activate the Emergency Plan. | Emergency Manager |
| 2 | **Gather steering group.**  Gathers a steering group to ensure maximum attention.  The Emergency Manager, who has activated the emergency plan, decides who, where and when. | Emergency Manager |
| 3 | **Define log responsibility.**  Appoint who will log responsible, and how to communicate to log responsible.  The emergency process must be documented on an ongoing basis. | Emergency Manager |
| 4 | **Status**  The steering group is briefed on the incident. Including how   * Impact on customer business * Technical impact Internal * Decision whether continuing in disaster mode. * Decision for Technical Lead and Commercial Lead * What has been done up to this time? * Alternatives at customer side * Alternative internal * Plan B * Information and communication   Note what has occurred, what is done, what is running and what is scheduled. | Emergency Manager |
| 5 | **Initiate management**  Call in Technical Lead and a Commercial Lead. | Emergency Manager |
| 6 | **Next activities**  Identify possible uses of emergency plans or action plans.  Agree on communication intervals and " next actions ". | Emergency Manager |
| 7 | **Communication**  Decide Internal communication and communication with customers, partners, etc. | Emergency Manager |

## 

## Second step during emergency

|  |  |  |
| --- | --- | --- |
| Step | Description | Responsible |
| 1 | **Possibly meeting with supplier (s)**  Technical and Commercial Lead meet with key supplier (s) to be involved.  It is decided how incident management takes place with supplier (s) and who communicates with Technical and Commercial Lead | Technical and Commercial Lead. |
| 2 | **Secure staffing at [the customer]**  Get an overview, who is working on Incident now and what skills are missing. Be sure to contact and activate additional staffing. | Technical Lead |
| 3 | **Meeting with emergency staffing**  A meeting is held (online) with the emergency staff at [the customer] to ensure that everyone is informed about the situation and ongoing activities. | Technical Lead |
| 4 | **Next activities**  Identify possible uses of emergency plans or action plans.  Agree on communication intervals and " next actions ". | Technical and Commercial Lead. |
| 5 | **Communication**  Internal communication and communication with customers, partners, etc. | Commercial Lead |

## Next steps during emergency

|  |  |  |
| --- | --- | --- |
| Step | Description | Responsible |
| 1 | **Status**  The Emergency Manager is briefed on the incident. Including how   * Impact on customer business * Technical impact internal * Decision whether continuing in disaster mode. * Decision for Technical Lead and Commercial Lead * What has been done up to this time? * Alternatives at customer side * Alternative internal * Information and communication   Note what has occurred, what is done, what is running and what is scheduled. | Emergency Manager |
| 2 | **Next activities**  Identify possible uses of emergency plans or action plans.  Agree on communication intervals and " next actions ". | Emergency Manager |
| 3 | **Communication** Decide Internal communication and communication with customers, partners, etc. | Emergency Manager |

# DATA LIST

## Roles and responsibility

Roles and responsibilities are defined in the table below:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Name | Title | E-mail | Phone | Escalation order | Decision responsible | Press handling | Technical Lead | Commercial Lead | Special task |
| Fill out with internal roles |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

## 

## Supplier

The following suppliers can be activated on standby as needed.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Supplier | Scope | Period of time | Reaction time | Contact info |
| IT Relation A / S | Service desk  Server infrastructure  Network infrastructure | 24X7 | 15 min at P1 | [Servicedesk@itrelation.dk](mailto:Servicedesk@itrelation.dk)  Tel. +45 *222222222*    Note critical cases must be submitted by telephone. |
| Supplier A | Navision | Mon- Fri 8-18 | 1 hour at P1 | Tel. +45 *333333333*    Note: IT Relation must contact the supplier directly. |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Critical systems

The list of critical systems is used for the emergency management's prioritization, so that it is ensured that the right systems are addressed first.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| System | Critical for | Servers | Dependencies | Contact for system validation |
| Rufus line (sample) | Receiving orders | Server232, Server121 | AD, Server432 |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## 

## Workarounds

Workarounds is used during the period when a system is not available. Work arounds can be activated by decision of the emergency management. Workaround is defined for the following systems:

|  |  |  |  |
| --- | --- | --- | --- |
| System | Expected time for establishment | Workaround | Contact person for commissioning |
| Rufus line (sample) | 30 min | Order Receipt Email  Described in "Emergency plan for Rufus line" |  |
|  |  |  |  |
|  |  |  |  |

The procedure for initiating Work arounds can be operationally described in separate documents, and there is a reference to documents in the section "Supplementary documents".

## Communication methods

The communication method depends on which communication channels work during the emergency. Method is decided by the emergency management based on the following:

|  |  |  |
| --- | --- | --- |
| Purpose | Method | How |
| First session of emergency management | Mobile phone (call)  Mobile phone (SMS)  Teams  Personal contact | The person activated by the emergency management ensures that the other emergency management is contacted and that a subsequent meeting form and time is agreed. |
| First activation of employees and specialists | Mobile phone (call)  Mobile phone (SMS)  Teams  Personal contact | Emergency management and / or Situation Management ensures that the necessary staffing is activated. |
| Communication during emergency situation | Mobile phone (call)  Mobile phone (SMS)  Teams (chat)  Teams channel  Personal contact  Email | Emergency management and / or Situation Management ensures that the necessary communication for emergency management and staffing is made on an ongoing basis. |
| Alternative communication method during emergency plan | WhatsApp is used for calls and chat group | Emergency management ensures that a WhatsApp group is activated and that it is communicated that WhatsApp is used (see separate instructions under "Supplementary documents" ). |

## Scenarios

Emergency can activate s in connection with different scenarios. The section here aims to list probable scenarios, as well as best practice for handling.

|  |  |  |
| --- | --- | --- |
| Scenario | Symptoms | Action |
| Denial of Service - attack | Network connection becomes unavailable, and / or large amount of traffic hits the network infrastructure. | Contact IT Relation and ask them to activate their action plan for Denial of Service - attack. |
| Ransomware - encryption | Systems become encrypted and inaccessible. | Contact IT Relation and ask them to activate their action plan for Ransomware - attack. |
| Other security incidents | Theft of data, accidental disclosure mm. | Use Procedure for handling security incidents.  And if IT Relation operates the affected systems, ask them to activate their Security Incident Procedure |
| Power outage in data center | No contact to systems at the location. | IT Relations must begin with analysis and plan for re-establishment. |
| Power outage location A | No power | Call supplier A |
| Power outage location B | No power | Call supplier B |
| Office location not available | Fire, explosion, water damage or similar. | [Customer] action |
| Pandemic | Major share of employees is sick and / or office location decommissioned. | [Customer] action |
| Large sections of infrastructure inaccessible | Large range of unavailability, hardware defective. | IT Relation handles this in their emergency plan |
| Entire infrastructure must be restarted / started | This may be necessary t, if there are many errors in the running system, and all systems are inaccessible. | See check list " Start-up order of [customer s ] -s systems ". *This must be made.* |
| Large parts of [customer s ] servers need to be re-established from backup | Files and systems are encrypted or corrupted. | Apply IT Relations procedure for recovery. Prioritize efforts based on "Critical systems" |
| *Critical systemA cannot be put into operation* |  | *Contact supplier 123* |
| *Critical systemB cannot be put into operation* |  | *Contact supplier 123* |

## Supplementary documents

The following documents can be found either at IT Relation or at [the customer]

|  |  |  |  |
| --- | --- | --- | --- |
| Document | Type | Location | Application |
| ITR - Situation Management Procedure | Procedure | This is described on IT Relation processes and security. | Is activated before emergency is activated. Situation Management can be chosen to continue throughout the emergency. |
| ITR- Procedure for managing and handling security incidents | Procedure | This is described on IT Relation processes and security. | Best practice for handling security incidents that ensure that you get through the right phases such as. collection of evidence. |
| ITR - Action Plan for Denial of Service | Action plan | This is described on IT Relation processes and security. | Operational plan for handling Denial of Service attacks. |
| ITR - Action Plan for Ransomware Attacks | Action plan | This is described on IT Relation processes and security. | Operational plan for handling Ransomware attacks. |
| Activating WhatsApp | Guide | This is located…. . | Guide to establishing WhatsApp as a communication method. |
| Handling Cybercrime | Guide | This is located… |  |
| Boot order [customer] s systems | Checklist | This is available:  ITR: i Vimana  Customer: ……. |  |
| Emergency plan - | Emergency plan |  |  |
| Emergency plan - | Emergency plan |  |  |
| Emergency plan - | Emergency plan |  |  |
| Emergency plan - | Emergency plan |  |  |

# GOVERNANCE

## Introduction and purpose

There is a great use and dependence on information technology at [the customer]. Availability, integrity, and confidentiality of business-critical systems are therefore essential for the business to function.

This emergency plan must support good handling of critical incidents for the company's IT Infrastructure. The emergency plan is targeted at managing the Incident and can thus apply to all extraordinary critical incidents that affect availability (crashes) and cybercrime incidents. The goal is to minimize inaccessibility, and for cyber-attack incidents in addition to limit the damage.

The emergency plan is built on the base of IT Relations' standard template for emergency plans, which gives the advantage that uniformity is ensured around roles, structure, activation etc. It provides the best possible prerequisite for successful use of the emergency plan in the collaboration between [the customer] and IT Relation. However, the emergency plan can also be used in an emergency that does not involve IT Relation.

## Scope

The emergency plan addresses the tactical and organizational aspects of dealing with an extraordinary critical incident where normal procedures and processes are not sufficient. The plan is targeted at [the customer's] IT infrastructure.

### Definition of a disaster:

* A significant event causing us and / or our customers to lose the ability to continue operation of their business.
* Definition note: A disaster applies only to loss of one operating center, as defined in the prepared contingency plan.
* Natural disasters: storm flood, flood, fire storm, hurricane, earthquake, snowstorm, etc.  
  Human-made: ex. Terror or war  
  Other: ex. Pandemic or key components that fail (logical and physical)

The above includes both cyber-attack incidents where top priority is to limit the damage, and critical crashes where top priority is to re-establish accessibility.

## Boundaries

The emergency plan is targeted at extraordinary critical situations where the incident cannot be controlled through normal measures such as Incident Management.

The emergency plan does not include the operational handling of specific critical incidents. Operational actions can instead be addressed in action plans and workaround plans, which will then be supplementary appendices to the emergency plan.

## Guidance in using the emergency plan.

This section is targeted at those who have a role as decision manager, Emergency Manager, Technical Lead or Commercial Lead (collectively referred to as the Emergency Management) defined in the emergency plan under "Roles and Responsibilities" and aims to provide a quick overview of the plan's content.

The following can thus guide the emergency management while the incident is active.

* Activation of emergency plan
  + The emergency management can expect to be contacted by the Company's employees or IT Relation Incident Manager in the event of a critical incident (described under Activation Criteria). See the section "Activation criteria" for a more detailed description. After this, the decision-maker in the emergency response decides whether the emergency response must be activated.
  + See the section Action descriptions and First step during emergency plan to get the first activities started correctly.
  + The Communication section supports how communication can take place by activating the emergency plan.
* Organization of emergency plan
  + Roles and responsibilities describe the roles that must be staffed, as well as responsibilities that lie in the individual roles.
  + Use the Communication section to help establish information during emergency plan.
  + It must be ensured that everyone is aware of their role and responsibilities.
* During emergency situation
  + The emergency management leads the incident to a solution and continuously ensures that sufficient and competent resources are activated and that there is clarity about status and activities.
  + Check which annexes are referred to under "Supplementary documents" for handling the incident, in relation to whether they are targeted at the specific incident.
  + See the section “Critical systems” as input for prioritization during emergency plan, as well as who can verify the system's functionality during re-establishment.
  + See the section “Scenarios” for handling specific scenarios. This section can be brief instructions or referral to operational emergency or action plans.
  + The Suppliers section shows a list of suppliers that can be activated as needed during the emergency.
* Guidelines on Emergency Plan and supplementary documents
  + This section is not relevant during an emergency, but contains guidelines for updating, knowledge, testing and lessons learned.

## Structure

Emergency management consists of the emergency plan itself and supplementary procedures and action plans.

|  |  |  |
| --- | --- | --- |
| Tactical level | **Emergency plan**  **Procedures** | Tactical approach to managing an incident. |
| Operational level | **Action plans**  **Emergency plans**  **Procedures** | Operational instructions which address a very specific incident. If these exist, they will be described in external documents. |

## Role descriptions

Decision responsible

* Appoint a Emergency Manager – maybe himself.
* Has decision-making competence in all respects during emergency plan. This also includes who is manning which roles.
* Decides on activating and deactivating emergency plan.

Press handling

* Must speak to the press and externally in general.

Technical Lead

* The role of Technical Lead must be staffed. Technical Lead drives and decides in relation to problem solving, resources, etc. Has the overall technical dialogue with Technical Lead at IT Relation.

Commercial Lead

* The role Commercial Lead must be staffed. Commercial Lead supports Technical Lead and handles the commercial dialogue with IT Relations, Customers and Partners (finance, law, general collaboration, etc.).

Special Task

* Participates in emergency plan for special tasks. This includes e.g. access to buildings, network specialists, security specialists, logging activities, support, etc.

The emergency management

* Decision responsible, Technical Lead and Commercial Lead are collectively referred to as the emergency management.

## Activation criteria

We work with the following criteria within emergency plan focus:

|  |  |  |
| --- | --- | --- |
| Operation works. There may be several open support cases, but none are priority 1 cases | Cat 1  Normal operation | Emergency plan deactivated. |
| We have a Major Incident, which means that critical system is not available. Resolution time is not expected to be more than 4 hours or there is control over the incident. | Cat 2  sharpened operation | It must be ensured that management has been escalated and that there is management of incident resolution.  The emergency management is informed by e-mail. |
| We have a Major Incident for Critical System. Redemption time is expected to be longer, or the event may develop further. We are not in control. | Cat 3  Serious situation  ??????? | Incident resolution is owned by incident management.  The emergency management must be contacted by telephone, and a decision must be made as to whether the emergency must be activated. |
| Critical and prolonged malfunctions or cyber-attacks to a violent extent. | Cat 4  Critical situation | Emergency plan is activated, and the emergency management takes over the management of Incident. |

In order for the emergency response to be activated, it is assumed that employees are aware that management must be scaled up in the event of critical incidents, and that the management is aware of this emergency response plan and when they must contact the emergency management.

It is always a decision-maker under the roles and responsibilities of the final decision, in relation to whether the emergency plan should be activated or whether the Incident should be treated on the basis of standard procedures. It must be ensured that relevant suppliers are informed that emergency plan is activated, so that they understand the priority for solution.

## Abandonment of emergency plan management

It is the Emergency Manager who decides to stop emergency plan.

Before the emergency response stops, it must be ensured that there is an overview of the situation, and that incident handling has come under control.

When the emergency response is stopped, communication is made internally and to affected customers and suppliers, so that everyone is aware that the emergency response has been stopped, and how it may further course is.

## Critical systems

Critical systems are defined as systems of [the customer] that are necessary for [the customer] to fulfill its obligations to its customers or regulatory obligations.

The list of critical systems is used for the emergency management's prioritization, so that it is ensured that the right systems are addressed first.

The table in the data list must serve as a basis for decision-making for actions for re-establishment and validation.

## Workarounds

Workarounds is used during the period when a system is not available. Work arounds can be activated by decision of the emergency management. Work around is defined for the systems in the data list.

The procedure for initiating Work arounds can be operationally described in separate documents, and there is a reference to documents in the section "Supplementary documents".

## Communication

Communication is an important part of emergency plan, as status and activities must be updated on an ongoing basis, and new decisions must be made. Communication is based on the guidelines in the data list.

## Communication methods

The communication method depends on which communication channels work during the emergency. Method is decided by the emergency management based on the following:

### Internal communication

First communication

As soon as possible after the emergency response has been activated, an internal communication must be made so that everyone at [the customer] is informed of the situation, roles and responsibilities, and that the emergency response is activated. Commercial Lead is responsible for internal communication. Initial communication internally is done via email (if available) and must include the following:

* Information that the emergency response is activated.
* Brief description of Incident (when it occurred, status, who / what is affected).
* Information on staffing the roles Technical Lead, Commercial Lead.
* Emphasize who can / may communicate externally.

Communication during the incident

Subsequently, the Commercial Lead is responsible for making internal communication at appropriate intervals (Standard interval is 1 time per hour). Ongoing communication should include:

* Status of the incident
* Next activities
* Key activities and rope holders on these
* Possibly. changes in emergency management.

Emergency communication Internal

Emergency communication internally can take place as a telephone chain, where top management ensures information to its managers. Leaders secure information for the next link, etc.

### 

### Communication with Suppliers for IT Infrastructure to be involved.

First communication

Inform that the emergency plan has been activated to suppliers who either need to be involved or may become involved. Initial communication internally is done via email, and should include the following:

* Information that the emergency response is activated.
* Information that the case is to be given top priority with the supplier.
* Brief description of Incident (when it occurred, status, who / what is affected).
* Information on staffing the roles Technical Lead, Commercial Lead.
* Questions about who can take a similar Technical Lead and Commercial Lead role with the supplier.
* Information about what is expected of the supplier, including expectations of 24X7 activities.

Communication during the incident

Commercial lead is responsible for ongoing communication. Interval is assessed according to the situation and the supplier's role in the emergency plan, and this is agreed with the supplier.

### External communication

External communication may only be performed by persons authorized for Press Management under "Roles and Responsibilities". In addition to the **Press,** external communication also includes:

* Customers
* Authorities

The task of external communication can be performed by other persons in the emergency response, but only after a decision from a person authorized to press handle.

## Scenarios

Emergency can activate s in connection with different scenarios. The section in the data list aims to list probable scenarios, as well as best practice for handling.

## Supplier

The suppliers in the data list can be activated on standby as needed.

In the event of a disaster must quickly establish s cooperation with these suppliers where appropriate.

## Supplementary documents

The documents in the data list can be found either at IT Relation or at [the customer]

# Guidelines on Emergency Plan and supplementary documents

## Who should know the emergency plan?

Everyone with a role defined under "Roles and responsibilities" must know the emergency plan, its purpose and their own role. It must be ensured that once a year a review of the emergency plan is made in its entirety.

Managers in [the customer] must be familiar with:

* There is an emergency plan.
* When should the emergency management be contacted?
* Who to contact (Decision makers)

The awareness of the emergency plan and the above points must be ensured at least once a year.

XXX is responsible for to ensure the Awareness and training.

## Test of emergency plan

The emergency plan must be tested once a year as an exercise based on an imaginary scenario. The test must be started in the delivery, where the scenario is activated, and continues, until the emergency management has been contacted and the emergency management has an initial meeting.

XXX is responsible for testing being further defined and added to the annual cycle.

## Lessons learned.

After an incident where the emergency plan has been activated and after testing the plan, a reflection must be made on points that can be improved. What works and what does not work. This aims to learn from a specific incident and continuously update and optimize the emergency plan.

## Availability and updating of the emergency plan and supplementary documents.

The following applies to the emergency plan as well as supplementary documents mentioned in the emergency plan.

* Update
  + For all updates, the history at the bottom of the document must be filled in with the version number and a short definition of corrections.
  + Documents must be updated regularly in the event of significant changes.
  + Documents must be updated at least once a year.
* Availability
  + Documents must be available electronically and at least in a printed set.
  + Current version must be available electronically on ……
  + The current version must be available in physical copy on….
  + After each update, a link to the current version is sent to everyone with a role defined under "Roles and responsibilities."

## Log guidance

A log of emergency plan activities must be kept. The log must be used for an overview during the emergency plan as well as for a subsequent investigation. The table below can be used for logging.

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Time | Responsible | Action |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## 

## Emergency plan history

|  |  |  |  |
| --- | --- | --- | --- |
| Dato | Revision | Author / responsible | Summary |
| 25-07-2022 | 0.1 |  | Emergency plan created |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Et billede, der indeholder tekst, græs, skærmbillede

Automatisk genereret beskrivelse

## Et billede, der indeholder tekst, skærmbillede, Font/skrifttype, design Automatisk genereret beskrivelse