**Guide to using   
Wired Relations' templates**  
Wired Relations' templates\* can be used directly in your work with data protection and information security - but can also be used as inspiration for your own material. You can modify them as needed to make them exactly as you want them.A black background with black lines

Description automatically generated

**NOTE!** There may be sections that are not relevant for all companies. If this is the case, it will be clearly indicated in the text.

|  | Text boxes in the document contain focus points and good advice. Please note that the text boxes should be removed  from the final version of the specific policy or procedure. |  |
| --- | --- | --- |

There will be places in the text where you are prompted to insert the company’s name or other information. In these cases, it will be marked as follows: *[insert company's name]*.

At the end of each document, there will be a table that provides an overview of the document's version, the latest update, and who is responsible for the document.

|  | Here are some additional tips for using Wired Relations' templates: |  |
| --- | --- | --- |
|  | * You can add or remove sections, change the wording, and add your own logo and branding. |  |
|  | * Stay up-to-date with your templates. Data protection and information security regulations are evolving rapidly, so it's crucial to keep your templates current. |  |
|  | Should you have any inquiries concerning the templates, please feel free to contact us. |  |

**IT Contingency Plan**

**1. Purpose**

The IT contingency plan ensures that the IT-dependent, business-critical processes in *[insert company's name]* can be restored reliably after a critical incident has directly or indirectly prevented normal operations.

The IT contingency plan itself contains role descriptions, instructions, and procedures to be followed in the event of an activation of the plan. This ensures a clear distribution of responsibilities and roles, so that responsible persons know what to do in a contingency situation.

**2. Scope**

The IT contingency plan includes the use of IT at *[insert company's name]* at the following location(s): *[Insert company location(s)]*.

If the use of IT at *[insert company's name]* is wholly or partly purchased as a service from a third party in an outsourcing agreement, including cloud solutions, then *[insert company's name]* must ensure that appropriate security measures have been agreed upon and implemented by the supplier in relation to recovery.

**3. Planning**

3.1 Objectives

*[insert company's name]* has set time-based objectives for the recovery of business-critical IT services, referred to as Recovery Time Objectives (RTO). The system list is up-to-date and is continuously maintained in *[e.g., Wired Relations - alternatively, the system list can be inserted as a table below or in an appendix]* with an indication of RTO (and possibly other relevant criteria) for each system.

|  | A prerequisite for setting RTO goals is that critical IT systems have been identified, and that a dialogue has taken place with the company's various departments/representatives regarding how long IT support can be dispensed with. This dialogue typically takes place in conjunction with the ongoing risk assessments.  RTO goals reflect the business requirements, which must be viewed in light of the security level the organization has decided on, the implemented security measures, and the operational processes of the contingency plan.  When setting RTO goals, considerations include whether there is a possibility of using alternative procedures for IT support (e.g., manual processes) and what current preventive measures have been implemented in critical IT systems to prevent failures (increase resilience). |
| --- | --- |

Recovery is considered complete when individual services are available to users and it is possible to maintain the daily IT operational support of the company.

3.2 Contingency premises

For systems covered by the IT contingency plan, the following points must be completed and updated at all times:

* Backup on disks (disk backup), including license keys, etc.
* Copy of the technical system descriptions
* Administrator passwords and other important usernames and passwords.
* Copy of the operating instructions

*[If relevant insert other relevant points, such as*

* *Copy of IT supplier agreements / operating agreements*
* *Copy of the list with prioritisation of systems (Which systems are to be restored first and which systems can wait till the end)]*

*[Describe where above is stored, e.g. in a fire-proof cabinet located in a different fire zone than the IT systems and/or stored in a secure, external location]*

| The purpose of this information is to be available even if the electronic versions are not. As far as possible, such a copy should be kept outside the company’s main office/location. Remember that this information is confidential and must therefore be protected and access controlled. |  |
| --- | --- |

3.3 Contingency activation

The IT Contingency Organization is activated when an incident cannot be handled within the framework of *[insert company name]*'s processes and procedures.

Contingency response must be activated when *[define the criteria for activation of the IT Contingency]*

|  | The decision to activate the IT contingency plan is always made on a case-by-case basis, but the following criteria typically serve as benchmarks. For example, if one or more of these criteria are met, or if there is a risk that they may be met.  Inspiration for defining criteria:   * **Duration of the incident**   + If there is a risk that an incident cannot be handled and resolved within the affected assets’ Recovery Time Objective (RTO), this constitutes a crisis requiring activation of the IT emergency response. * **Significant data loss**   + If an incident is of such a nature that it may result in a greater data loss than the company's tolerance for loss, this may indicate a crisis requiring activation of the IT emergency response. * **Extent of impact**   + If a significant portion of the company's IT infrastructure is affected by an incident, this may indicate a crisis requiring activation of the IT emergency response. * **Special events**   + Natural disasters (earthquakes, floods, etc.) may require activation of the IT Contingency Organization.   It is essential that employees are informed about the reporting channel to be used in the event of a detected incident (or suspicion thereof). |
| --- | --- |

**4. Contingency Organization**

| In small companies, the roles can be combined in the “CEO”. In medium-sized companies, roles may be distributed among different individuals, such as a coordinator, IT manager, communications officer, etc.  Different roles and responsibilities that may be included in the IT Contingency Organization are described in the table below.  **This table should be adapted to the specific situation and organization of the company.** |
| --- |

4.1 - Roles and Responsibilities

The roles and responsibilities/tasks within the contingency organization are described below to clarify and visualize the tasks of each role in a crisis situation.

| **Role** | **Task** |
| --- | --- |
| IT Contingency Management | *[Example description****:*** *The IT Contingency management team is the highest authority for all decisions related to the operational handling of an emergency crisis. The IT emergency management team serves as a forum for discussing significant management decisions regarding the operational handling of the emergency crisis.]* |
| IT Contingency Coordinator | *[Example description: The IT Contingency coordinator creates and maintains the incident log, assists management, and ensures coordination of individual activities..]* |
| Communications Officer | *[Example description: The company's external stakeholders must be informed of the situation and ongoing progress. Describe who the company's stakeholders are, e.g., employees, customers, partners.].* |
| Recovery Teams | *[Example description: The company's external stakeholders must be informed of the situation and ongoing progress. Describe who the company's stakeholders are, e.g., employees, customers, partners.].* |
| Supplier Roles | *[Example description: If there are specific roles agreed upon with the supplier, these should be described here. For example, this could include contact persons at the supplier.]* |

Below is a contact list for the Contingency organization, as well as for other parts of the company that may be involved.

4.2 Contact Lists

| **Contact list for the Contingency organization** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Role** | **Position** | **Name** | **Address** | **Email / phone number** | |
| *IT Contingency Management* | *e.g. CEO* |  |  |  | |
|  | *e.g. CISO* |  |  |  | |
|  | *e.g. DPO* |  |  |  | |
|  |  |  |  |  | |
|  |  |  |  |  | |
| *IT Contingency Coordinator* | *e.g. Information security coordinator* |  |  |  | |
| *Communications Officer* | *e.g. Communications Director* |  |  |  | |
|  |  |  |  |  | |

| **Contact list for other departments in the company** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Role** | **Position** | **Name** | **Address** | **Email / phone number** | |
| *Department A* | *e.g. Manager* |  |  |  | |
| *Department B* | *e.g. Manager* |  |  |  | |
|  |  |  |  |  | |
|  |  |  |  |  | |

| **Contact list for suppliers** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Role** | **Position** | **Name** | **Address** | **Email / phone number** | |
| *Supplier A* | *[insert]* |  |  |  | |
| *Supplier B* | *[insert]* |  |  |  | |
| *Network Provider* | *[insert]* |  |  |  | |
|  |  |  |  |  | |

4.3 Meeting Place for the IT Contingency Organization

If it is not possible for the IT Contingency organization to meet at the company's usual location *[insert meeting place at the company's location]*, when the contingency plan is activated, an alternative meeting place has been agreed upon.

*[Insert alternative meeting place].*

**5. Alerting and assessment**

All alarms within normal working hours are sent to the *[insert relevant contact person]*, who assesses the severity of the problem that has arisen.

Contact number: xxxx xxxx

(also see the contact information in Section 4.2)

In the event of damage to the physical framework, contact *[insert relevant contact person]* during normal working hours. The building manager is then informed and makes the final decision

All alerts about serious incidents outside normal working hours are made to the *[insert relevant contact person]*, who then assess the extent of the problem

Notification of a serious incident must be forwarded to *[insert relevant contact person, e.g. the IT Contingency Management cf. Section 4.2]*, who makes the final decision on the activation of the contingency response.

5.1 Assessment

*[Insert relevant contact person, e.g. the IT Contingency Management cf. Section 4.2]* assesses the situation and investigates internally (or with the supplier) how long it will take to restore the damage, and based on the criteria in section 3.3, decides whether to activate the IT contingency .

Service providers are notified of a potential contingency situation.

### **6. Maintaining the IT Emergency Response Plan**

### 6.1 Testing

The IT Contingency plan must be tested at least once a year to ensure that it is effective and that the IT Contingency Organization is familiar with it.

*[Describe how you test the IT Contingency plan].*

| The type and extent of testing required should be determined on a case-by-case basis.  One example is to conduct a tabletop exercise once a year. This test is conducted based on a predefined scenario. A tabletop exercise tests parts of the IT Contingency plan, such as the escalation process and the accuracy of contact lists. A tabletop exercise does not involve disrupting IT operations.  In addition to a tabletop exercise, a full test of one or more action plans can be performed, where one or more systems are restored. This can be done, for example, every two or three years.  If any deficiencies are found in connection with testing of the IT Contingency plan and in the period between detection and remediation, it is essential that the deficiency is stated in the IT Contingency plan, as it may be critical for the IT Contingency Organization during a possible incident.  Deficiencies can advantageously be stated in, for example, an appendix to the IT Contingency plan. |
| --- |

All tests of the IT Contingency plan are documented, including any identified deficiencies and the plan for remediation/update.

### 6.2 Updating the IT Contingency Plan

The IT Contingency plan must be updated at least once a year following the annual test of the IT Contingency plan. The IT Contingency plan should also be updated if there are significant changes in the use of IT, supplier changes, restructurings, or changes in the IT Contingency organization.

### 

### 6.3 Distribution and Storage

The IT Contingency plan must be stored so that it is always accessible in an emergency situation, which means that it is not sufficient to store it electronically. Each member of the IT Contingency organization should keep a physical copy of the plan. The person responsible for maintaining the IT Contingency plan is also responsible for distributing the latest updated version to all recipients.

An overview of distributed copies can be maintained below:

| **Receiver** | **Role** | **Location/storage** | **Comments** |
| --- | --- | --- | --- |
| *Name* | *E.g. CEO* | *[Insert address and location]* | *[E.g. stored physical]* |
|  |  |  |  |
|  |  |  |  |

### **7. Action Plans**

Action plans are designed to assist the IT Contingency organization in managing a specific incident, including ensuring that all procedures and steps to be taken in the event of an activation are followed.

The course of events is documented in the incident log (Appendix 6).

It is important to note that action plans are merely a supporting tool. The IT Contingency organization must always assess the specific situation and take the necessary actions.

Specific action plans can be found in Appendices 1-5. A template for the incident log is provided in Appendix 6.

|  | Examples of specific action plans can be found in Appendices 1-5 below. These plans should be adapted to the specific needs of the company.  Additional action plans may be required, such as:   * A plan for a new location (to ensure a quick and efficient transition to a new location) * A plan for hardware restoration (to support the process of procuring new equipment to restore IT operations) * A plan for network restoration (to ensure adequate network access is restored)   It may also be necessary to develop checklists, such as a checklist for normalized operations. |
| --- | --- |

**Appendix 1 - Physical incidents (fire, water, explosion, etc.) that put the office out of operation**

**(EXAMPLE)**

**Description:**

The action plan describes the physical contingency and IT contingency that must be put in place if *[insert company name]’* premises are completely or partially destroyed, to such an extent that the normal routines cannot handle the re-establishment of IT operations.

For example, this can be in the event of fire, water damage, explosion, etc.

**Documentation:**

Upon activation of the contingency plan, all activities must be logged for subsequent documentation - use the incident log in Appendix 6. It is also important to describe any identified weaknesses or vulnerabilities in the IT contingency plan or systems. An evaluation should be conducted to determine if this necessitates changes to systems or procedures

**Assumptions:**

*[Outline the prerequisites for this action plan. There will often be conditions necessary for the successful implementation of the plan, such as equipment, agreements, physical locations, logistical considerations, or specific skills. For example, a prerequisite could be the availability of “basic infrastructure” (phones, internet, etc.)]*

| **No.** | **Action** | **Responsible** |
| --- | --- | --- |
| 1 | Ensure the safety of personnel, premises, equipment, and other assets. Contact the landlord or other stakeholders as necessary. | *[insert responsible according to section 4.1]* |
| 2 | **Activate a temporary location if required**  If a relocation is necessary, this process should be initiated. | *[insert responsible according to section 4.1]* |
| 3 | **Communication**  Communicate the situation to all employees and determine if employees should work from home until the temporary location is re-established. If necessary, forward calls to other phones. | *[insert responsible according to section 4.1]* |
| 4 | **Repair any damage to the primary location** | *[insert responsible according to section 4.1]* |
| 5 | **Reestablish IT operations**  When re-establishing the server room, determine if IT systems can be restored to the same equipment or if new equipment needs to be procured. (A separate plan for hardware procurement may need to be developed.) | *[insert responsible according to section 4.1]* |
| 6 | **Verify that the primary location can be used and that IT operations have been restored**  Ensure that everything is ready for use. Network connections are re-established. Necessary systems and data are accessible. The premises comply with labor law requirements before being put into use. | *[insert responsible according to section 4.1]* |

**Appendix 2 - IT incidents affecting a central system (EXAMPLE)**

**Description:**

The action plan describes the IT contingency that must be established if a central IT system becomes completely or partially inaccessible and the IT operations do not appear possible to re-establish within the system's defined Recovery Time Objective (RTO).

**Documentation:**

Upon activation of the contingency plan, all activities must be logged for subsequent documentation - use the incident log in Appendix 6. It is also important to describe any identified weaknesses or vulnerabilities in the IT contingency plan or systems. An evaluation should be conducted to determine if this necessitates changes to systems or procedures

**Assumptions:**

*[Outline the prerequisites for this action plan. There will often be conditions necessary for the successful implementation of the plan, such as equipment, agreements, physical locations, logistical considerations, or specific skills. For example, a prerequisite could be the availability of “basic infrastructure” (phones, internet, etc.)]*

| **No.** | **Action** | **Responsible** |
| --- | --- | --- |
| 1 | **Activating the IT Contingency Plan**  Relevant personnel are called in/assembled. | *[insert responsible according to section 4.1]* |
| 2 | **The affected system is shut down** | *[insert responsible according to section 4.1]* |
| 3 | **Restore**   * It is determined whether the IT system can be restored on the same equipment or if it needs to be restored on different equipment, which would then be procured. Alternatively, the IT system environment can be re-established in a virtual environment with an IT provider. * A timeline for the restoration of normal operations is created. The estimate is continuously reviewed and updated, and the status is communicated to relevant stakeholders (management, employees, etc.). | *[insert responsible according to section 4.1]* |
| 3.1 | **Activate operations**  Using the restore, operations of the affected systems are reactivated, and it is verified that:   * Systems are ready for operation. * Data is not corrupted. * Network connections are re-established.   During the restoration process, the IT contingency organization collects any documentation related to the problem that may be relevant for subsequent assessment of the root cause, in addition to what is already available in logs, etc. | *[insert responsible according to section 4.1]* |
| 4 | **Communication**  Once the problem is resolved and everything is ready for operation, this is communicated to relevant stakeholders (management, employees, etc.). | *[insert responsible according to section 4.1]* |

**Appendix 3 - Virus and hacking attacks (EXAMPLE)**

**Description:**

The action plan outlines the preparedness that needs to be established if the IT infrastructure is compromised by a virus or hacking attack.

**Documentation:**

Upon activation of the contingency plan, all activities must be logged for subsequent documentation - use the incident log in Appendix 6. It is also important to describe any identified weaknesses or vulnerabilities in the IT contingency plan or systems. An evaluation should be conducted to determine if this necessitates changes to systems or procedures

**Assumptions:**

*[Outline the prerequisites for this action plan. There will often be conditions necessary for the successful implementation of the plan, such as equipment, agreements, physical locations, logistical considerations, or specific skills. For example, a prerequisite could be the availability of “basic infrastructure” (phones, internet, etc.)]*

| **No.** | **Action** | **Responsible** |
| --- | --- | --- |
| 1 | **Activation of IT Contingency organization**  Relevant persons are being called in/assembled | *[insert responsible according to section 4.1]* |
| 2 | **Initial assessment**  First, an assessment is made as to whether to start with additional logging and tracking (capture of traffic and memory dumps).  This is to gain certainty of what;   1. is going on, 2. get better clues of who has gained access, 3. as well as to be certain that there is no logical bomb.   Furthermore, it is assessed whether it may be an internal attack, where it may be appropriate to isolate a person or a group from further work.  If deemed appropriate, networks with infected systems are isolated, i.e., the network connection is interrupted and, if possible, virtual systems are paused. | *[insert responsible according to section 4.1]* |
| 3 | **Evaluation of extent**  An assessment of the extent of the attack is made, including whether it will be possible to re-establish operations on other equipment that, in such case, is procured. The IT system environment can be re-established in a virtual environment with an IT provider if necessary.  It is also assessed how an IT defence can be maintained or restored, including managing security until normal operations are re-established. If necessary, contact your telecommunications/internet service provider and/or relevant authorities for assistance. | *[insert responsible according to section 4.1]* |
| 4 | **Time estimate for restoration**  A preliminary time estimate is prepared for the restoration of normal operation. The estimate is reassessed on an ongoing basis and this, as well as the status, is announced to relevant stakeholders (management, employees, etc.). | *[insert responsible according to section 4.1]* |
| 5 | **Notifications to relevant stakeholders**  It is ensured that appropriate notifications to relevant external stakeholders, including briefing of any customers whose security may have been affected is made. If customers may have been affected, these are offered technical assistance to counteract this. | *[insert responsible according to section 4.1]* |
| 6 | **Handling**  The infected systems are assessed and examples of the virus, the attack pattern, etc are collected. If the virus is known and there is an existing cleaning routine, attempts are made to remove the virus, otherwise external antivirus partners are used to remedy the infection.  At the same time, logs from the firewall, proxy, system logs, etc., are reviewed to find the source of the infection. If it is assessed that the source of infection can be identified as an external customer/partner, they must be notified of the attack. | *[insert responsible according to section 4.1]* |
| 7 | **Reviewing all systems**  Once the attack is neutralised, all systems must be reviewed to ensure that:   * The systems are ready for operation (consider backup of systems before possible restore) * Data is not corrupted * Network connections have been re-established. | *[insert responsible according to section 4.1]* |

**Appendix 4 - Events affecting the cloud-based IT services (EXAMPLE)**

**Description:**

The action plan describes the IT contingency plan that must be established if one or more cloud-based IT services become completely or partially unavailable and it does not appear to be possible to re-establish operations within Recovery Time Objective (RTO)

**Documentation:**

Upon activation of the contingency plan, all activities must be logged for subsequent documentation - use the incident log in Appendix 6. It is also important to describe any identified weaknesses or vulnerabilities in the IT contingency plan or systems. An evaluation should be conducted to determine if this necessitates changes to systems or procedures

**Assumptions:**

*[Outline the prerequisites for this action plan. There will often be conditions necessary for the successful implementation of the plan, such as equipment, agreements, physical locations, logistical considerations, or specific skills. For example, a prerequisite could be the availability of “basic infrastructure” (phones, internet, etc.)]*

| **No.** | **Action** | **Responsible** |
| --- | --- | --- |
| 1 | **Activation of IT Contingency organization**  Relevant persons are being called in/assembled | *[insert responsible according to section 4.1]* |
| 2 | **Evaluation of extent**  An assessment of the extent of the problem is carried out, including what is needed to re-establish the affected operation and whether it is necessary to establish alternative solutions. If necessary, contact the telecom/internet provider and/or relevant authorities for assistance.  If it is deemed necessary to establish an alternative solution, this will be dealt with in the first instance - see step 3. | *[insert responsible according to section 4.1]* |
| 3 | **Restore**  It is clarified whether it is possible to restore the IT system on the same equipment or whether it should be done on other equipment, and if so such equipment is procured. Possibly, the IT system environment can be re-established in a virtual environment with an IT provider**.**  During the work of re-establishing operation of the affected systems, the IT contingency Organization collects any documentation of the problem that may be relevant for the subsequent assessment of the cause of the problem, in addition to what is already in the logs, etc. | *[insert responsible according to section 4.1]* |
| 4 | **Time estimate for restoration**  A preliminary time estimate is prepared for the restoration of normal operation. The estimate is reassessed on an ongoing basis and this, as well as the status, is announced to relevant stakeholders (management, employees, etc.). | *[insert responsible according to section 4.1]* |
| 5 | **Communication**  When the problem has been rectified and everything is ready for operation again, this is reported to relevant stakeholders (management, employees, customers etc.). | *[insert responsible according to section 4.1]* |
| 6 | **Reviewing all systems**  Once the attack is neutralised, all systems must be reviewed to ensure that:   * The systems are ready for operation (consider backup of systems before possible restore) * Data is not corrupted * Network connections have been re-established. | *[insert responsible according to section 4.1]* |

**Appendix 5 - Communication (EXAMPLE)**

**Description:**

The action plan describes a communication plan that can be used if the IT- contingency Organization is activated.

**Documentation:**

Upon activation of the contingency plan, all activities must be logged for subsequent documentation - use the incident log in Appendix 6. It is also important to describe any identified weaknesses or vulnerabilities in the IT contingency plan or systems. An evaluation should be conducted to determine if this necessitates changes to systems or procedures

**Assumptions:**

*[Describe the prerequisites that apply to this action plan. There will often be conditions necessary to be able to implement the action plan, such as equipment, agreements, physical locations, logistical conditions or competencies. An example could be "Basic infrastructure (telephony, internet, etc.) is available.]*

| **No.** | **Action** | **Responsible** |
| --- | --- | --- |
| 1 | **Develop a Timeline**  A timeline for both internal and external communication will be developed. | *[insert responsible according to section 4.1]* |
| 2 | **Gather Information**  All information required for internal and external communication will be gathered by the designated communication person. | *[insert responsible according to section 4.1]* |
| 3 | **Determine Communication Channels**  For each individual internal and external communication, the communication channel will be determined. | *[insert responsible according to section 4.1]* |
| 4 | **Develop External Messages**  If external communication is required, materials will be developed and approved by the IT-contingency Organization. | *[insert responsible according to section 4.1]* |
| 5 | **Translate Relevant Documentation**  If it is necessary to attach documentation, translations will be made as needed. | *[insert responsible according to section 4.1]* |
| 6 | **Disseminate Information**  Ensure that all internal and external communication is disseminated simultaneously, if required, and that the messages are consistent. | *[insert responsible according to section 4.1]* |
| 7 | **Respond to Questions**  Respond to any questions, focusing on the most critical questions and stakeholders. | *[insert responsible according to section 4.1]* |

**Appendix 6 - Incident Log (EXAMPLE)**

Contingency plan: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Start date: \_\_\_ / \_\_\_ - 20\_\_\_

| **Start** | **End** | **Noted by** | **Activity** | **Approved by:** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Document information**

| Document version |  |
| --- | --- |
| Date of Issue for this version |  |
| Responsible Person |  |
| Status |  |