|  |
| --- |
| **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.

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

|  |
| --- |
| Text boxes in the document contain focus points and good advice for you as a data controller or data processor. 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 organization's name or other information. In these cases, it will be marked as follows: [insert organization's name].

At the bottom 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:

* Read the instructions carefully before you start using the templates. This will help you understand how to use them effectively.
* Customize the templates to fit your organization's needs. You can add or remove sections, change the wording, and add your own logo and branding.
* Keep your templates up to date. Data protection and information security regulations are constantly changing, so it's important to make sure your templates are always up to date.

We hope you find Wired Relations' templates helpful. If you have any questions, please don't hesitate to contact us.

**IT Contingency Plan**

**1.1 Purpose**

The IT contingency plan aims to ensure that the IT-dependent business-critical work processes in [Insert Organization Name] and the affiliated companies can be re-established and are functional after a critical incident has directly or indirectly prevented normal process execution for a longer period.

The IT contingency plan itself contains role descriptions, instructions, and procedures that must be followed if a contingency is activated. In particular, emphasis has been placed on the fact that the plan tells which overall activities must be initiated and who is responsible for them. In this way, the employees and specialists who are activated in the individual scenarios described in the appendices can concentrate on solving the tasks/problems they are confronted with.

At the same time, it is clear who the contact person is for each area when there is a need for it.

The IT contingency plan must also ensure that the individual plans always reflect the current situation. This means that several background tasks must be carried out at regular intervals so that the premises for the plan are updated.

**1.2 Objective**

The document must always be updated so that documentation, procedures, etc., always reflect the company's current situation.

**1.3 Scope**

The IT contingency plan covers IT use at [Insert Organization Name] at the location(s) where the company currently has its physical presence.

If IT use at [Insert Organization Name] is wholly or partly purchased as a service from a 3rd party in an outsourcing agreement, including cloud solutions, then [Insert Organization Name] must make a separate assessment of whether the outsourcing agreement is appropriate in relation to [Insert Organization Name]'s needs and requirements for re-establishing IT use.

The IT contingency plan does not cover other causes of business interruption such as major outbreaks of disease, e.g. food poisoning or illness among staff. This should be included by [Insert Organization Name] as part of [Insert Organization Name]'s general terms and conditions, for example, as force majeure.

The IT contingency plan does not cover the re-establishment of the office environment, work production premises or how [Insert Organization Name] conducts business during and after an incident.

**2. Contingency Preparation**

The IT contingency plan must be activated when one or more incidents disrupt or interrupt critical parts of [Insert Organization Name]'s business processes for a longer period of time and the processes cannot be restored under normal operation and troubleshooting within the specified time horizon, which is 24 hours.

* Physical incidents (fire, water damage or other) that put [Insert Organization Name] out of operation, wholly or partly.
* IT incidents that affect a central system.
* IT incidents that affect [Insert Organization Name]'s IT infrastructure (virus outbreaks and hacker attacks).
* IT incidents involving the compromise of [Insert Organization Name]'s systems with a risk of data leakage, where others may gain unauthorized or unintended access to information.
* Incidents that only affect the cloud-based IT services used by [Insert Organization Name], e.g. [Insert relevant systems].

**2.1 Contingency Premises**

For systems covered by the IT contingency plan, the following steps must be carried out and updated at all times:

* Backups on discs (disc backup), including license keys, etc., are stored on an external, secure location.
* Copy of the technical system descriptions
* Administrator passwords and other important user names and passwords.
* Copy of operating instructions

Please also refer to point 2.1.7, which states that this IT contingency plan can also be found as an electronic copy on the management/board's laptop.

**2.1.1 Contingency Activation and Re-establishment Requirements**

The IT contingency plans describe:

* who is responsible for activating a contingency, the conditions for activation and how activation should take place
* which facilities must be available when a contingency is to be activated
* communication to employees, partners and customers, including a description of alternative communication channels

**2.1.2 Contingency Situations**

The IT contingency plans cover the following situations:

* establishment/activation of IT contingency
* operation under IT contingency (IT contingency operation)
* normalization of the situation

**2.1.3 Activation Decision**

Contingency must be activated:

* when an incident is assessed to have a long-term and/or destructive nature for IT use
* when it can be immediately ascertained that there is extensive destruction of premises and IT systems
* if there is an assessment that there is a risk of data leakage, either as an independent incident or as part of another incident

When IT contingency comes into effect, IT contingency management has the first priority with regard to access to all resources in [Insert Organization Name].

Security Measures in [Insert Organization Name]

**2.1.4 Prerequisites**

It is assumed that:

* There is access to ongoing backup of the system, databases, and data.
* [Insert Organization Name]'s rules are known to internal and external parties involved in an IT contingency situation.

**2.1.5 Testing the IT Contingency Plan**

The IT contingency plan must be tested at least once a year. This can be done as a desk test. A desk test is a test in which management reviews and assesses whether the IT contingency plan is adequately described and can be considered to cover management's expectations for re-establishing IT use. The test may cover all or selected parts of the IT contingency plan.

**2.1.6 Updating**

The IT contingency plans must be updated at least once a year, or when there are major changes in [Insert Organization Name]'s technical or business organization.

The IT contingency plans are available on [Insert Organization Name]'s shared drive and are distributed to the persons mentioned above. They all receive the new versions.

**2.1.7 Storage**

The IT contingency plan, with its associated technical documentation and annexes, etc., is stored on encrypted drives on the management/board's portable IT equipment. The purpose is to ensure that the material is available in the event of IT failure or lack of access to [Insert Organization Name]'s premises. For this reason, at least some of the management's portable IT equipment should be stored outside of [Insert Organization Name]'s premises.

**3. Contingency Instructions - Alerting and Roles**

**3.1 Alerting**

All alerting during normal working hours must be done directly to management, who will assess the severity of the problem that has arisen.

Contact phone number: [Insert phone number]. (See contact information in section 3.2.1)

In case of damage to the physical facilities, management must be contacted during normal working hours. The facility manager will then be informed and make the final decision.

Serious incidents must be reported directly to [Insert Organization Name] management.

Management will make the final decision on whether to activate the contingency plan.

**3.2 Responsibilities and Role Allocation**

Responsibilities and roles include the following tasks:

**The CEO (Management):**

The CEO, alternatively the rest of the board:

* Is a member of the responsible crisis management team. The crisis management team is responsible for ensuring that the contingency plans are provided with the necessary resources, both in terms of personnel and finances.
* Is responsible for all communication, including internal information on status, etc.

It is therefore important to remember that:

**All communication with customers, the press and others must be through the CEO or board of directors.**

**IT Contingency Management:**

[Insert relevant position in the organization], alternatively the rest of the board:

* Is directly responsible and coordinating for the correct implementation of the IT contingency plan
* Is responsible for the technical operation and documentation of systems, backups, etc.

**Building Manager:**

**The CEO**, alternatively the rest of the board:

* Is responsible for the physical framework, including communication lines, power, etc.
* Is also responsible for communication with the landlord.

**Technical Staff:**

Provides the necessary technical resource for IT contingency:

*[Insert relevant position in the organization]* and internal IT

**Other staff:**

Provides support for IT contingency if necessary.

**3.2.1 Contact/Phone Numbers**

* The CEO *[Insert name and phone number]*
* *[Insert relevant position in the organization as well as name and phone number]*
* *[Insert relevant position in the organization as well as name and phone number]*

### **Document Information**

|  |  |
| --- | --- |
| Document Version |  |
| Date of Issue for This Version |  |
| Responsible Person |  |
| Status |  |