

Safety regulations for the prevention of cyber loss, S711

Your obligation to prevent damage, valid as of 1 January 2024

Welcome to the safety regulations!

In these safety regulations, we explain what your business must do and take into consideration to prevent cyber loss.

❗ Read the regulations carefully. If you do not comply with the regulations, we may reduce or deny your insurance compensation.

These safety regulations are part of your insurance contract.

Your insurance contract consists of the policy document, insurance terms and conditions, safety regulations, and the general contract terms and conditions.

The **policy document** lists your company's insurance policies and the terms and conditions applicable to them.

The **insurance terms and conditions** describe the terms under which your property is insured.

These safety regulations describe your obligations to prevent damage.

Pohjola Insurance's general terms of contract contain general provisions related to your insurance.

We interpret the policy document, insurance terms and conditions, safety regulations, and general contract terms and conditions as a whole.



Policy document



Insurance terms and conditions



Safety regulations
This document



General Terms of Contract

CONTENTS

1	Purpose of the safety regulations: prevention of cyber loss	2
2	Required measures to prevent and limit damage	2

1 Purpose of the safety regulations: prevention of cyber loss

The purpose of these safety regulations is to reduce the number of cyber loss cases and decrease the damage they cause. In these regulations, cyber loss refers to loss or damage caused by a data system break-in, denial of service attack, malware or a data security breach. In the worst case, cyber loss can endanger the continuation of your company's operations.

Your business has an obligation to ensure that

- the safety regulations are followed in all activities carried out by the policyholder, insured persons or parties comparable to insured persons
- those responsible for performing the work or otherwise responsible for preventing damage are familiar with the content of the safety regulations.

2 Required measures to prevent and limit damage

Quality and access rights of processed data

- ✓ **Identify** which information is vital to your company's operations regarding its availability, confidentiality and integrity.
- ✓ **Classify** information based on its quality and related obligations.
- ✓ **Process** personal data in accordance with the Data Protection Act and EU's General Data Protection Regulation.
- ✓ **Appoint** a Data Protection Officer if your company processes personal data and when required by legislation on data protection
- ✓ **Determine** who has the need and right to access which information, and who handles the access rights.

Backup copies

- ✓ **Ensure** that all your company's data is backed up daily.
- ✓ **Store** the backup copies so that the original data and the copies cannot be corrupted at the same time.
- ✓ **Encrypt** the information on the backup copies if necessary.
- ✓ **Check** every three months that the backup system works as planned and the information is up to date.
- ✓ **Ensure** that the above obligations are part of the service agreement if a third-party service provider is responsible for the backup copies

Data security and its maintenance

- ✓ **Make** sure that every device and network part uses firewall and anti-virus programmes.
- ✓ **Ensure** that the devices can be locked and information encrypted, including in mobile devices.
- ✓ **Enable** automatic updates for software whenever possible
 - **Update** software regularly if it has no automatic updates.
 - **Check** for updates at least once a month.
- ✓ **Organise** data security training for your personnel. The content and amount of training depends on the quality and quantity of the data your company processes.
- ✓ **Ensure** that information is removed from any decommissioned devices permanently, and that all devices are disposed of or recycled securely.

- ✓ **Make** sure that remote connections only use a secured connection and multi-factor authentication for the system or service
 - Example: When an employee logs in to the company's network using a remote connection, they will use the secure VPN connection and identify themselves with a username, password and at least one additional means of identification.
- ✓ **Take** care that the wireless network of your company is secure, and the wireless network for guests or customers is separate from your company's own network.
- ✓ **Use** the help of a third-party professional if you are unable to fulfil the obligations mentioned in these safety regulations.

By following these regulations, you will ensure occupational safety and avoid unpleasant surprises in the event of an insurance claim.

Thank you for taking the time to read these safety regulations!

Pohjola Insurance Ltd, Business ID: 1458359-3

Helsinki, Gebhardinaukio 1, 00013 OP, Finland

Domicile: Helsinki, main line of business: non-life insurance companies

Regulatory authority: Financial Supervisory Authority, www.fiva.fi