Pohjola Insurance

Cyber insurance safety regulations

Safety Regulation S711, valid as of 1 April 2020

1 Purpose

These safety regulations are to be included in the insurance contract to supplement the actual insurance terms and conditions. These safety regulations include technical safety regulations and advice which, provided that they are complied with, may prevent loss and damage from occurring and diminish their volume.

2 Obligation to comply with safety regulations

These safety regulations are part of the insurance agreement. Both the policyholder and the insured must comply with the safety regulations and its provisions. If the safety regulations are not complied with, the compensation may be reduced or completely denied in accordance with the Insurance Contracts Act.

The policyholder must ensure that people working in the company are familiar with the contents of these safety regulations.

The cyber security instructions are designed to primarily help small and medium-sized organisation that may not have enough resources to hire their own or external cyber security staff, and to assess and improve their cyber risk management.

3.Cyber security instructions

3.1 Development and maintenance of information security policy

Organisations must specify and document their information security policy or supplement their existing policy to cover at least the following areas:

Classification of data and information systems

How data is classified, what kind of data security must be followed when handling data of different levels, and what kind of information systems are used to handle data.

The roles and responsibilities related to information security

The information security policy must define clearly the information security roles and responsibilities: who is responsible for information security, who is the Data Protection Officer, who is authorised to process data of certain level, who is in charge of the information security of systems and repositories, and how access rights are managed.

Handling and protecting personal data

If an organisation collects personal or customer data, the information security policy must specify the operating models for processing personal data in accordance with the Personal Data File Act and the EU General Data Protection Regulation.

Instructions for use of social media and data networks

The information security policy contains instructions and restrictions for the employee's use of social media and data networks.

Maintenance and updates

The information security policy must define how it is maintained and updated and the party who will approve any changes. It must also specify how the policy is brought effectively to the attention of the employees and other relevant stakeholders.

The information security policy and any supplementary information security instructions may also include a more detailed description of the matters presented in sections 3.2-3.11.

3.2 Information security and privacy protection

The organisation must be clear about at least the following in terms of information and information security:

- What kind of data does the organisation use and store in its operations: customer data, account data, data about financial transactions, contact details, data related to purchase behaviour, bank contact details, credit card details, salary information, tax information, personal data, health data, patient information, proprietary and sensitive business information and other confidential information about customers, employees or other stakeholders.
- How is this data processed and protect.
- Who has access to the data and under what conditions. Who needs to access confidential data to perform their work duties, and who does not need to access confidential data. What levels of use and access rights do various people have to the data.

- Which information systems or data are critical for business continuity.

Based on the above, data should be categorised, in terms of confidentiality, into the following categories, based on the vm.fi/VAHTI guidelines:

- Top secret
- Secret
- Confidential
- Restricted access
- Public

Once data has been categorised, user rights and information security principles must be specified for each category under the basic principle that the more sensitive and critical the data is, the fewer people should have access to it and the better it should be protected (by means of, for example, passwords, encryption and, if necessary, physical identification devices or biometric identifiers).

The policyholder must ensure on a daily basis that up-to-date backups exist of all files. Backup copies must be kept in a separate physical location than the original data, and backups must also be encrypted if necessary.

Data backup must be arranged so that any data that is critical to the operations should be possible to be recovered from the backups when necessary. Backup recovery must be regularly tested to ensure that the backup and the recovery processes are functioning. It must be specified who is in charge of performing backups, what data is backed up, using what equipment, how often, how backups are stored, and who has access to the backups.

Operating instructions must be in place in case of data theft or loss of data and these instructions must be made available to all who process or use data.

3.3 Employee's information security practices

Appropriate rights to use data and information systems must be defined for the employees depending on their work roles. Persons who have no need to process confidential data in their work should be denied access to it. If a certain task requires the processing of confidential data, each person's access rights must be determined case by case and restricted only to such data and systems that are required for performing the task.

No customer data or other confidential data may be accessed without a work-related reason. Such data may not be handed over to third parties unless it is absolutely certain who that person is and that the person is authorised to access the data.

Always use secure data transfer methods and any data that is sent to a public email account must be encrypted if necessary.

Confidential data (either in electronic format or as a paper copy) must only be kept for as long as it is needed or regulations require it to be kept. Any disposal of data, because it is outdated or for any other reason, must be carried out in a secure way.

All employees must follow a clean desk policy so that any documents containing confidential information may not be seen by anyone visiting the premises.

All employees must undergo information security training covering the organisation's information security policy, safe use of information technology and the most important information security risks and tools for managing them. Refresher courses must be arranged regularly and whenever there is relevant information about new information security threats or procedures.

Operating practices must be established to ensure that persons no longer working for the organisation will cease to have access to the systems and data immediately once their employment relationship has ended.

3.4 Fraud and scams

Electronic data transfer and the internet offer criminals many new ways to engage in fraud and scams towards organisations and their customers. Some crimes of this nature are not covered by cyber insurance but by traditional crime insurance. The key methods for protection against fraud and scams include:

- if you receive suspicious email messages, do not open any attachments or click any links in them
- do not install any software if you are not sure about its operation, purpose or origin. Only administrators should have the rights to install software.
- the operating system, virus protection, firewalls and other software must always be updated with the latest security patches. Automatic updates must be used for all software whenever possible.
- employees have been trained to recognise phishing and social engineering
- the identity of persons asking for personal data on the phone must always be checked by ringing them back to a number that is known to be their valid number
- customers have been told that they will never be asked to give confidential, private information (passwords, bank account details, payment card details etc.) over the phone or by email
- unnecessary use of USB flash drives or other portable data storage devices is avoided, and they are always virus checked
- links in website pop-up windows shall not be clicked in order to avoid spyware

3.5 Network security

The organisation's network must be separated from the public network with firewalls and proxy servers in all public network interfaces. Virus protection software and software that can detect attempts to break into the system must be used in all interfaces if necessary to have sufficient security controls.

If cloud services are used, it must be ensured that the service provider offers at least as good protection to data as your own network. It must be ensured that the service

agreement has defined the service provider's responsibilities, service levels, recovery times, any backup services and the option to audit the service.

Password practices that require employees to use sufficiently strong passwords must be established (instructions can be found on the website of the Finnish Communications Regulatory Authority). The passwords or phrases should be changed regularly and be only known by the users themselves.

Access to the wireless local area network (WLAN) must be limited to devices and users specified by the organisation. WLAN encryption should be WPA2 level.

If a wireless network is available for guests, it must be separate from the organisation's own network, so that the organisation network's data and applications cannot be accessed through the guest network.

Any secret and confidential data should be encrypted whenever possible. If the company has a website, its protection must be ensured.

Any systems and software in the network must be updated with latest software versions and updates whenever they become available. Automatic updates should be used especially for virus protection, prevention of malicious software and firewall software.

Access to websites which employees do not need for their work duties should be prevented. Browser settings must be adjusted to prevent access to forbidden websites through the internal network.

If remote access connections are used, their data security must be taken care of. Remote access connections must be secure and have strong two factor authentications using either hardware or software tokens.,

The information security policy must bring to the attention of everyone that unidentified USB flash drives or other portable data storage devices may not be connected to computers or mobile devices linked to the network before checking them for any malicious software.

3.6 Security of home pages and web servers

Web servers providing data and services for customers are among the most common targets for cyber-attacks. Web servers, their operating systems and related network infrastructure must be carefully protected against cyber-attacks, denial of service attacks and any other inappropriate use.

When designing a web service that is open to customers, the security resources required have to be taken into account. It must be ensured that the hardware and software solutions enable a sufficient security level and that there is enough expertise to maintain and update it.

When implementing a web service, it must be remembered that the factory settings of hardware and software have often been pre-set with ease of support and speed of use in mind, not necessarily considering a sufficiently high level of security. The system's security settings should be carefully checked and changed wherever necessary to meet the organisation's needs. It is particularly important to change all the default passwords to strong ones that meet the requirements of the organisation's information security policy and to ensure that the latest security updates have been installed. Unnecessary services, applications and content should be removed from the online service. The information security of online services and content should also be tested.

It should also be ascertained that the online service only publishes relevant, necessary and appropriate information. If confidential data or personal data must be published on the service, a particularly high level of security must be maintained. Whenever necessary, sensitive data must be encrypted and user authentication must be sufficiently secure.

The integrity of data published in the online service must be checked. It must be ensured that unauthorised use or tampering of data has been prevented sufficiently well.

The web server's security maintenance requires regular procedures for which sufficient resources must be reserved, such as:

- maintenance and analysis of log data
- installation and testing of the latest updates and patches
- regular backups of critical data
- recovery procedures in case of disruptions
- regular testing of online service security.

3.7 Email security

Email is a critical part of daily operations in many organisations. At least the following must be taken into account in terms of email security:

Spam filters and virus protection must be used to check all email. It must also be ensured that the filters and virus protection are automatically updated to their latest versions. The spam filter settings must be checked regularly so that they will not prevent the receipt of necessary email.

All employees using email must be trained to the secure use of email. The employees must identify risks of using email and understand when and how email can be used for work duties and when expert help should be sought.

Confidential information shall be emailed only to persons who are authorised to use it. It must be specified what kind of information can not be emailed and what must be encrypted.

3.8 Mobile devices

At least the following should be taken care of with regard to the security of mobile devices:

Use of information security applications on all mobile devices

All phones and tablets should have security software installed and in use, if any is available for them.

Software updates

Similar to any fixed workstations, all mobile devices should have the latest software versions, especially regarding security software.

Use of passwords on phones and other mobile devices

If possible, strong passwords should be used on mobile devices in the same way as on fixed workstations. Mobile devices must be set to lock automatically if they are not used for a while.

Encryption of data on mobile devices

Data on mobile devices must be encrypted to prevent it from being accessed if the device is lost or gets into the wrong hands.

Observing the environment

Users of mobile devices must prevent any confidential data or passwords from being seen by outsiders.

Use of email and social media on mobile devices

The same security regulations apply to both mobile and fixed devices with regard to email and social media.

Operating model if mobile device is stolen or lost

An operating model must be established in case a mobile device is stolen or lost. Users must know what to do in order to deactivate the device and protect the data in it.

Deleting data from mobile devices no longer used

When devices are no longer used, it must be ensured that all data is irrevocably deleted from them. Any SIM cards no longer in use must also be disposed of in a secure way.

3.9Facility and operational security

Regarding facility and operational security, at least the following must be taken into account:

Arranging the physical security of the premises to minimise the risk of device theft and information leaks

Data-processing equipment that is easy to take along (laptops, tablets, smart phones) must not be kept in areas that can be accessed from public places. If necessary, equipment may be locked with a cable if it must be kept in a place that is easy to access. Tracking programs may also be installed on the devices.

Keeping user identifiers and passwords near the workstations and other devices must be forbidden.

Screens where confidential data is shown must be placed in a way that they cannot be viewed from areas where outsiders have access.

Securing confidential material that is printed out

Printing out confidential material should be avoided as much as possible. Printouts must be kept in lockable filing cabinets or safes. Printers used for printing confidential material should be equipped with software requiring user identification to prevent printouts from being left lying on the printer or its vicinity.

Letter post security

Information security procedures must be established also for the sending and receiving of letter post. Confidential letter post must not be subjected to conditions where its data security can be jeopardised.

Secure disposal of trash

Trash containing confidential information must be disposed of in a secure way. Procedures must be in place for shredding material containing confidential information or collecting such material in locked containers until they are shredded.

Any confidential information in computers, tablets, smart phones or data storage devices to be disposed of must be purged in a secure way, just deleting the files is not enough.

3.10 Payment information security

If an organisation offers the option of card or online payments to its customers, the security of data stored to perform these must be ensured. Typically, the service for card and online payments is provided by an external service provider, which also processes the card and payment information and ensures their security. If an organisation stores data about the customer, cards or accounts during payment in, for example, the client register, such data must be processed in a secure way at all stages of the process. If any card numbers and customers' personal information collected for other than payment purposes can be replaced with other identifiers, this should definitely be done.

Only equipment and software approved for payment system use may be used. Outsiders must be prevented from accessing payment terminals, so that they cannot install skimming devices on them to copy card details.

The organisation's own payment transactions may only use approved payment transfer software or applications. Access to payment applications must be limited to persons who need to make payments as part of their work duties. If payment systems must be used remotely, the connections must be secured.

The provider of the payment service may in most cases give more detailed instructions on the secure methods of using payment systems and software.

3.11 Preparing against information security breaches or cyber attacks

In order to prepare against information security breaches or cyber attacks, operating models and instructions must have been specified and documented to enable appropriate and timely response to any data security breach.

The operating model must cover different types of cyber threats, such as: device theft; breakage or loss of equipment; system intrusion; malicious software; viruses; denial of service attacks; data theft; accidental data leaks; and cyber extortion.

For more information about the requirements concerning preparation against information security breaches and deviations, see the Government Information Security Management Board's (VAHTI) instructions website, for example document 8/2017 Management of data security breach situations or a more recent version of it.

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, finanssivalvonta.fi/en

Pohjola Insurance