Acceptable Use & Information Security Policy

English Version – V1.0

1 Table of contents

2 Policy information

2.1 Version history

Date	Version	Author	Change description
28/03/2018	0.1	Dominiek Leenknecht	Initial version
23/04/2018	0.2	Dominiek Leenknecht	Small adaptations after internal reviews
02/05/2018	1.0	Dominiek Leenknecht	Published version

2.2 Overview

Televic's intentions for publishing an **Acceptable Use & Information Security Policy** are not to impose restrictions that are contrary to Televic's established culture of openness, trust and integrity. Televic is committed to protect its employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, printing and other devices, storage media, network accounts providing electronic mail, WWW browsing, FTP or other connection methods, as well as the data that are created, processed or stored on these systems are the property of Televic. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every Televic employee, consultant and other affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

2.3 Purpose

The purpose of this policy is to outline the use of

- computer equipment
- data and information
- physical security systems

at Televic. These rules are in place to protect the employee and Televic. Inappropriate use exposes Televic to risks including virus attacks, compromise of network systems and services, legal issues and general tangible or intangible protection issues.

2.4 Scope

This policy applies to the use of information, electronic and computing devices, network resources and physical security systems to conduct Televic business or interact with internal networks and business systems, whether owner or leased by Televic, the employee or a third party. All employees, contractors, consultants, temporary and other workers at Televic and its subsidiaries are responsible for exercising good judgement regarding appropriate use of information, electronic devices, network resources, information on these systems and physical security systems in accordance with the Televic policies and standards and local laws and regulation.

This policy applies to employees, contractors, consultants, temporaries and other workers at Televic, including all personnel affiliated with third parties. This policy also applies to all equipment and security systems that are owned or leased by Televic, as well as to the information on these equipments.

3 Definitions & terminology

Term	Description
ICT Infrastructure	This term means all network infrastructure and other physical ICT related devices that are property of or used by Televic (data centers, servers, storage, desktops, laptops, printers, telephony, mobile devices, …). For the purposes of this policy, also all internal and external ICT applications and services that are managed by Televic or on behalf of Televic. This way, systems for access on distance (e.g. VPN), cloud services (e.g. Office 365, Sharepoint Online, …) are also included.
ICT administrators	All responsibles for the support and the good functioning of the ICT infrastructure, centrally managed (Televic Group, responsibility of the CIO) as well as decentrally managed (business units, responsibility of the General Manager or other countries, responsibility of the Country Manager).
ICT department	The ICT administrators that are responsible for central management of ICT infrastructure. This team is part of Televic Group and under responsibility of the CIO.
Authorized user	Every person that is allowed to make use of the Televic ICT Infrastructure. A distinction can be made between: • users with a normal Televic account (employees, management, board of directors, registered consultants or students, …) • users with a temporary account for wifi access • other users that get specific access, based on a specific management decision

4 Authorized and unauthorized use of the ICT Infrastructure

4.1 Authorized activities

The Televic ICT infrastructure may be used for **authorized activities that take place in the normal operational context of Televic, in particular research and development, supply chain, commercial activities and the activities that support all of these**. This implies the following (non-exhaustive list):

- Extensive use for personal or recreational purposes is not allowed;
- The ICT infrastructure may not be used to make personal gains or conduct a personal business;
- Any use that violates any applicable law or legislation, is forbidden;
- The ICT infrastructure may not be used to distribute confidential information knowingly and on purpose further than to the entitled recipients;
- It is only allowed to grant access to the Televic ICT infrastructure to persons or systems that are validated and approved by the ICT department. Therefore, every new user of the ICT infrastructure (whether this is an internal employee or an external party, like a consultant or student) must be announced to the ICT department on timely basis and user credentials and/or a computer system must be requested by means of the Infrastructure Helpdesk System[1].
- Violations of (security) policies or terms of use of internal or external computer systems are forbidden.

[1] https://it-support.televic.com/

4.2 Unauthorized information

The ICT infrastructure may not be used to spread **unauthorized information**. As unauthorized information is considered (non-exhaustive list):

- Information that calls for racism, xenophobia, discrimination, …;
- Information that is in conflict with public order or good morals;
- Information that is abusive, defamatory or offensive, including sexually explicit, discriminatory, defamatory or libelous material;
- Bullying, hate speech or calls to ciolence;
- Gambling or participating to lotteries or on-line casino games;
- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations.

4.3 Privacy law

When using the Televic ICT infrastructure, the European as well as the Belgian **Privacy Legislation** must be respected. This also means that the privacy of the users, more specifically the confidentiality and integrity of their private data and the privacy of their communication may not be violated:

- It is not allowed to read the electronic mail in the personal mailbox or the non-shared files (in particular those on the personal disk space or backup in the cloud) of another user without his unambiguous consent.
- When data from a particular user need to be accessed by other people, there must be taken care of that these data are on a shared disk or in a shared mailbox.
- Access to private data is only allowed based on individual exceptions on court order or at the request of State Security.
- Logging and monitoring of metadata of communication and files (like filenames, filesize, date of creation, access date, …) is not regulated in the same strict way. These metadata are accessible for employees of the ICT Department in order to be able to deliver the necessary supporting services.
- Exceptional access to data of persons that are temporarily or definitively incapable of acting (e.g. in case of a heavy accident, coma, decease, …) fall outside the scope of this chapter and is handled on an ad hoc basis in consultation with the HR Department and the Televic General Management.
- When an employee is leaving the company, this employee needs to clean up his private mailbox as well as the private drives on his computer. When the employee has left the company, the mailbox (containing the remaining emails) is converted into a shared mailbox, so do to drives on the user's computer. This shared mailbox and drives are made available towards the employees who are following up the business of the leaving employee. On top of this, an Out-Of-Office notification is activated on the converted mailbox, acknowledging contacts that this employee has left the company.

4.4 Copyright and other IP rights

When using the Televic ICT infrastructure, **copyright and other intellectual rights** must be respected. This also implies that copyrighted material and software may not be distributed or copied when this is in conflict with the copyright or the license terms.

4.5 Installation and use of software

The user is only allowed to **install and use software** on the devices that are part of the ICT infrastructure of Televic under the following conditions:

- All applicable copyrights and/or license conditions have been correctly met, in other words the effective use must be in accordance with the license conditions (e.g. some personal licenses may not be used in a commercial or business context);
- The associated information security risks were assessed with appropriate care and deemed acceptable, or reduced to an acceptable level with due diligence (e.g. through secure configuration or safety tests);
- If the user wants to use software that doesn't meet these conditions, he must look for alternatives that do;
- In case of doubt, the user can submit an inquiry via the Infrastructure Helpdesk System to verify whether specific software may be installed and used or not on the Televic infrastructure.

4.6 Security breaches

It is strictly forbidden **to commit security breaches** on the Televic ICT infrastructure, on the systems that are linked to or communicate with this infrastructure, or on any other external computer system and the internet[2]. Some examples are (non-exhaustive list):

- To force access to systems to which you are not authorized (even if these systems are insufficiently secured) and attempts to do so;
- To bypass internal and external system and network security;
- To intercept information that is meant for others, e.g. by capturing network traffic via a fixed network connection or by means of wireless devices;
- To pretend to be another user, e.g. by logging in and working with the account data of another user without his permission (with the understanding that the user who shares his account data one way or another with someone else, violates the information security policy; see 5.3).
- To develop, install, (try to) execute or (try to) spread malicious software (e.g. malware) with bad intentions on the Televic ICT infrastructure.

To avoid data security breaches, users are not allowed to connect external data storage media to their computer (e.g. USBs, external hard disks, …). When this is, however, required from a business continuity point of view (e.g. back-up from customer setup, data that need to be transferred to a system out of the Televic network, …), it is mandatory that the data on the external storage are encrypted.

PS. For R&D purposes, certain of these activities might be allowed, within a clearly defined framework and on a shielded network that is or is not linked to the Televic network infrastructure. In that case, the ICT department must always be informed via the Infrastructure Helpdesk System.

4.7 Identify vulnerabilities

It is forbidden to **search for vulnerabilities** in the protection and security of the Televic ICT infrastructure, even with good intentions ("ethical hacking").

[2] Also see the Belgian Act of 28 November 2000 on cyber crime

- Exception: ICT administrators (centralized as well as decentralized) have the responsibility to actively search for vulnerabilities of systems and applications under their responsibility and to remediate. This search and remediation might be delegated to a specialized party.
- If a user discovers a vulnerability (e.g. by accident) in the Televic ICT infrastructure, this vulnerability must be reported as soon as possible by means of the Infrastructure Helpdesk System to the ICT department. The exploit or further propagation of such vulnerabilities is considered to be unauthorized and unacceptable.

4.8 Connection to Televic network

- Within the buildings of Televic, only authorized computers and systems may connect to the ICT infrastructure by means of an UTP cable, with an IP address that is assigned automatically of by the ICT department according to the existing procedures.
  To guarantee the proper functioning of the network, the assignment of fixed IP addresses and hostnames is centrally managed by the ICT department.
- Within the buildings of Televic, only authorized computers may connect to the Televic wireless domain network, giving them access to other devices and applications on this domain (servers, applications, …). Therefore, every domain user must be announced to and approved by the ICT department, see 4.1.
- Within the buildings of Televic, any computer or device may connect to the Televic wireless guest network (“Visitors”). This network only gives access to the internet.
- Outside the buildings of Televic, only approved devices are allowed to connect to the Televic domain network by means of VPN.
- Outside the buildings of Televic, only approved users with a Televic account are allowed to connect to Televic services and applications in the cloud (e.g. Office 365, Sharepoint Online, …). This can be done by means of authorized as well as unauthorized devices.
- All systems that make use of the Televic ICT infrastructure or that connect to this infrastructure, wired as well as wireless, must be adequately and sufficiently secured. Devices that cannot meet this requirement (e.g. legacy systems that cannot be updated) may never be connected to the Televic network.
- With a view to the proper functioning and the security of the ICT infrastructure and in particular the Televic network, it is only allowed to change the structure or the configuration of the Televic network with permission of the ICT department. The installation of additional active network components requires the explicit permission of the CIO or his delegate.
- The ICT department provides and manages all WiFi wireless access points; the installation of own wireless access points is strictly forbidden.

5 Responsibilities of the users

5.1 Televic account

Users with a **Televic account** gain access to the Televic ICT infrastructure on the basis of a user name and password. The Televic account is an important part of the digital identity of the user and must be protected with appropriate care.

Therefore, it is forbidden to reveal your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

It is also strictly forbidden to save any password in a visible or easily detectable way (e.g. sticky note on your computer monitor).

5.2 Televic email address

A **personal Televic email address** is linked to the Televic account. This email address is the official communication channel between the user, Televic and the other parties doing business with. The corresponding mailbox must be consulted by the user on a regular basis.

Postings by employees from a Televic email address to newsgroups or social media should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Televic, unless posting is in the course of business duties.

The Televic personal email address may not be used to send unsolicited emails, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam). The same applies to creating or forwarding chain letters, Ponzi schemes or other pyramid schemes of any type.

5.3 Protect account

A Televic account is strictly personal. The user is responsible for the account that is assigned to him/her and for what happens under that account, except when the user has become – despite appropriate care – victim of abuse of the concerning account.
For the **protection of the Televic account**, a.o. the following rules must be carried out in accordance with the information security policy:

- The user must select a strong password (or a strong password sentence) that must be updated at least once per year[3].
- The password must be kept strictly secret. Login details of the own account may not be passed on to other persons, not even to close co-workers. When it is necessary to access an application with more users but only one account, a shared account must be requested by means of the Infrastructure Helpdesk System.
- When suspicion exists that a password has become known internally or externally, the compromised password must be replaced immediately[4].
- The re-use of the same password of the Televic account for other services, internal or external, is forbidden.
- It is not allowed to let others make use of your personal account. When, for practical reasons, a violation of this rule cannot be avoided, a temporary exception can be tolerated, awaiting a final and correct solution. This exception must be registered as soon as possible via the Infrastructure Helpdesk System.
  Employees cannot be asked to pass their account data to another person.

[3] The strong password as well as the yearly renewal are technically enforced.
[4] https://it-support.televic.com/KB/View/4963-how-to-change-your-active-directory-password

- When a computer is left unattended, even for a short time, this computer must be locked or signed out. This applies both for computers that are managed by the ICT department as for other devices (tablets, smartphones, …).

5.4 Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorised access or loss of information, Televic enforces a **clear desk and screen policy** as follows:

- Personal or confidential business information must be protected using security features provided for example secure print on printers.
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Care must be taken to not leave confidential material on printers or photocopiers
- All business-related printer matter must be disposed of using confidential waste bins or shredders

5.5 Working Off-Site

It is accepted that laptops and mobile devices will be **taken off-site**. The following controls must be applied:

- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
- Laptops must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used.
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

5.6 Appropriate care

The ICT infrastructure that is made available by Televic must be **handled with appropriate care** by the users. This implies a.o.:

- When a user detects a defect or a malfunctioning of a part of the ICT infrastructure, this must be reported by means of the Infrastructure Helpdesk System or to an ICT administrator.
- Televic ICT resources may not be left in an irresponsible manner and thus be exposed to the risk of theft or misuse.
- In accordance with the practical guidelines of the information security policy, all users and ICT administrators must actively take responsibility for the security of the available ICT infrastructure.
- All information security incidents (e.g. misuse of an account, malware infection, theft of devices or data, data breach with personal data or confidential information, … (non-exhaustive list)) must be reported by means of the Infrastructure Helpdesk System as soon as possible.

5.7 Backup personal disk space

Each user disposes of a OneDrive For Business account in the cloud. This account needs to be used to automatically take a backup of personal folders containing relevant personal or company data. The user can add or remove computer folders to be backed up with this solution[5].

The goal of this backup: when the computer of the user gets lost (e.g. theft) or unusable (e.g. disk crash), all the relevant documents can be downloaded easily on another machine.

This OneDrive account is linked to the Televic account.

5.8 Think before you click

Avoid websites that provide pirated material. Do not open an email attachment from somebody or a company that you do not know. Do not click on a link in an unsolicited email. Always hover over a link (especially one with a URL shortener[6]) before you click to see where the link is really taking you. If you have to download a file from the Internet, an email, an FTP site, a file-sharing service, etc., scan it before you run it. A good anti-virus software will do that automatically, but make sure it is being done.

All email attachments from external parties are automatically scanned by a threat emulation software[7]. When the user receives an external email with attachment, this attachment is replaced by a safe version (attachment where macro's, hyperlinks, … are disabled). In that case, a header is added in the email, allowing the user to download the original attachment after a thorough scan/sandbox emulation.

6 General Data Protection Regulations (GDPR)

6.1 Global principles

To comply with EU GDPR[8], Televic must observe the eight 'General Data Protection Regulation principles', ensuring that:

- Personal data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under this Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

[5] https://it-support.televic.com/KB/View/2603-onedrive-setup
[6] http://en.wikipedia.org/wiki/URL_shortening
[7] https://www.checkpoint.com/products/sandblast-office365-security/
[8] https://www.eugdpr.org/

- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

In practice, it means that the Televic must:

- have legitimate grounds for collecting and using the personal data;
- not use the data in ways that have unjustified adverse effects on the individuals concerned;
- be transparent about how they intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- handle people's personal data only in ways they would reasonably expect; and
- make sure they do not do anything unlawful with the data
- not share any personal data with subcontractors without written consent of the customer or without taking measures to anonymize the data shared

Personal data is information that relates to an identifiable living individual that is processed as data. Processing amounts to collecting, using, disclosing, retaining or disposing of information. The General Data Protection Regulation principles apply to all information held electronically or in structured paper files.

Sensitive personal data is information that relates to

- race and ethnicity,
- political opinions,
- religious beliefs,
- membership of trade unions,
- physical and mental health,
- sexuality
- criminal offences

Sensitive personal data is given greater legal protection as individuals would expect certain information to be treated as private or confidential – for example, a Televic employee may have a Televic email account that is made publicly available on the company's website whereas their home email account is private and confidential and should only be available to those to whom consent had been granted.

It is important to differentiate between personal information that individuals would expect to be treated as private or confidential (whether or not legally classified as sensitive personal data) and personal information you can make freely available. For example: the Televic employee's identity is personal information but everyone would expect it to be publicly available. However, the Televic employee's home phone number would usually be regarded as private information.

6.2 What should each employee do?

Whenever an employee wants to store personal data on the company network, this employee needs to inform the ICT department via the Infrastructure Helpdesk System.

In that case, the ICT department will take the necessary actions to

- verify that the data were collected in a GDPR-compliant way

- guarantee that the data are stored on a GDPR-compliant location (incl. auditing, access control, data breach monitoring, …)
- log this personal data storage or processing

When an employee wants to store personal data on an external resource (e.g. web service provider that offers safe storage), the employee must also inform the ICT department to make sure that at least logging of this data storage or processing is handled.

This should allow the ICT department to inform the necessary parties in case of a data breach and/or to easily retrieve the necessary data whenever an individual wants to carry out one of his GDPR-guaranteed rights

6.3 Individual rights

The General Data Protection Regulation includes the following rights for individuals:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

The General Data Protection Regulation entitles an individual the right to request the personal information Televic holds on their behalf – this is known as a Subject Access Request (SAR) and includes all and any information held by Televic, not just that information held on central files or electronically, so it could also include correspondence or notes held by others in Televic.

- SARs must be responded to within 1 month of receipt.
- The SAR should be made in writing by the individual making the request.
- Televic can refuse or charge for requests that are manifestly unfounded or excessive
- Parents can make SARs on behalf of their children if the children are deemed to be too young or they have consented to their parents doing so on their behalf.

Employees need to know and understand:

- How to manage, keep and dispose of data
- When they are allowed to share information with others and how to make sure it is kept secure when shared.

6.4 HR related data

6.4.1 Candidates & recruitment

- When candidates contact Televic for a specific vacancy, the information they send to Televic (CV and motivation letter) are only saved for the necessary duration of the application process. At least one month after closing of this vacancy, these documents are get rid of.

- When a candidate with the right competencies is not selected for a vacancy, the HR department informs the candidate that Televic would like to keep his data for future opportunities. Only if the candidate agrees, the above mentioned documents are kept for a longer time, limited to maximum 2 years.
- Recruitment and application feedback data are logged in a protected database (only accessible by recruitment team). These historical data are maintained and never get rid off, the candidate also doesn't have the right to be informed on the contents of this information. This decision is based on the GDPR principle of "legitimate interest".

6.4.2 Employee data

All employee personal data are stored in an external payroll system[9]. The employee has access to this platform by means of a specific personal account. The employee can review this information on the payroll portal. The employee doesn't have the "right to be forgotten" for these data, since Televic needs to be able to prove wage payments etc. for a time period of at least 7 years.

Therefore, an ex-employee can at soonest request Televic to get rid of all the information that is linked to him when he has left the company for at least 7 years.
The same applies to evaluation data.
Both of these decisions are based on the legitimate interest principle.

7 Access control

This chapter only applies to the Televic HQ buildings in Izegem.

7.1 Alarm settings

The Televic building is equipped with an alarm system. The alarm system is inactive:

- on working days
- from 05:45 until 21:00

On all the other moments (at night, during weekends and during holidays), the alarm system is activated.
Only employees with an approved security code can activate or inactivate the alarm manually.
Each alarm code is unique and linked to exactly one owner. A user is not allowed to share his alarm code with other people.

Users that think to be eligible for an alarm code, can request such a code via the Infrastructure Helpdesk System.

When the alarm settings need to be adapted exceptionally (e.g. because of a company event or because overwork is due to meet project deadlines), this also needs to be requested as soon as possiblevia the Infrastructure Helpdesk System, at last at 4pm (16:00) on the applicable day.
Be aware that these settings cannot be overruled from a distance. This means, for example, when you have requested that the doors must remain open until 10pm (22:00), and the event has finished earlier (21:00), that at least one person must stay in the buildings until the requested time, since the doors are programmed to remain open for the fixed time period.

[9] https://dots.attentia.be/

7.2 Use of badges

All employees receive a badge when they start working in Televic Headquarters. This badge needs to be returned when the employee quits the company.

The badge is needed to open any external building door that is not under visual control, as well as some internal doors to protected areas (e.g. server room).

For most employees, the badge can only be used between 7am (07:00) and 8pm (20:00) + not in the weekend. For exceptional access outside these timeslots, the employee can request a 24/7 badge at the reception.

Everybody can always exit the building without badge via the underground parking (manual button). Opening a badge-protected door in an alternative way (e.g. with a screwdriver) is considered as burgling and therefore not allowed. Legal steps can be taken in case of such actions.

8 Compliance

By accepting an account or by making use of the Televic ICT infrastructure, the user commits himself to comply with these regulations. This regulation therefore also applies to external, occasional users of the Televic network.

9 Supervision, control and sanctions

9.1 Logging and monitoring

The Televic ICT infrastructure is controlled by the ICT department (logging and monitoring) to ensure proper operation and to trace and prevent abuse. The level of detail of this logging and monitoring may not be more and the retention time may not be longer than required to reach this goal.
The ICT department can also take the necessary measures to enforce this Acceptable Use Policy (e.g. by blocking specific internet traffic).
The logging and monitoring is executed in accordance with CAO 081[10] (Belgian privacy regulation).

9.2 Controlling authority

The Televic CIO has the controlling authority for the secure processing of personal data in Televic.

9.3 Audit

The CIO reserves the rights to audit networks, systems and users on a periodic basis to ensure compliance with this policy

9.4 Infrastructure Helpdesk System

The reporting of issues and incidents happens with the Infrastructure Helpdesk System[11], which acts as first point of contact and also as referral point towards other authorized channels, e.g. the CIO or this delegate.

[10] https://www.privacycommission.be/sites/privacycommission/files/documents/cao-081.pdf
[11] https://ict-support.televic.com/

9.5 Protective measures

In case of issues or incidents, the ICT department can decide to take protective technical measures with the goal, and limited to that, to protect the ICT infrastructure and its proper functioning.

9.6 Measures and sanctions

Possible measures and sanctions that can be taken against individuals in the event of active, deliberate and repeated infringements of this policy and taking into account the seriousness of the infringement, are:

- Disciplinary measures by the management: the temporary inactivation of an account or the temporary restriction of access to (parts of) the ICT infrastructure (where a balance is sought between the importance of the service, the protection of the systems and the rights of the person concerned, since the account might be indispensable for the execution of the job);
- Measures and sanctions as provided in the applicable regulations of Televic (e.g. work regulations).