Yettel.

INFORMATION SECURITY REGULATIONS FOR CONTRACTED PARTNERS

Yettel.

LOCAL MANUAL
Information security regulations for Contracted Partners

Owner: *Head of Information Security Office*
Approver: *Business Security Director*

Content

Yettel.

1 Purpose

This Local Manual contains the basic specifications for users who create, store, or process information from Yettel Magyarország Zrt. (hereinafter referred to as Yettel) and / or use Yettel information systems. The purpose of this Manual is to define the most significant information security regulations to be observed by users. Specifically applies to those users who are not Yettel employees but have access to Yettel assets (e.g., contractors, consultants, suppliers etc. – hereinafter “Contracted Partners”).

2 Scope

This Manual is valid for all users with access to data or information systems of Yettel without geographical limitation.

3 Basic regulations for Contracted Partners

3.1 The permitted use of information tools of Yettel

The information tools of Yettel - including all network access and resources (e.g., the Internet), all applications (e.g., email, chat) and collaborative tools (such as conference calls, video conferencing), shall not be used in breach of the Yettel Ethics Handbook, the Privacy Policy, the Information Management Policy or any other applicable Yettel policy or contract.

3.2 Prohibited use of information tools

Unauthorized use of information systems of Yettel or any attempt of that kind is strictly prohibited. It also applies to the unauthorized access and the manipulation and/or spread of information of Yettel. **Passing user’s data to other users or the use of other employees’ user data or the attempt of that kind (e.g., username, password, PIN) is strictly prohibited and will result in disciplinary action, up to and including the termination of contract.**

3.3 Data handling

Private information may be handled by Yettel according to the procedures of internal investigations and by the permission of Data Protection Officer. In case of private information handling contracted partners must comply with Data Processing Agreement (DPA).

Yettel business information can only be forwarded, processed and/or stored in devices or information resources which are not under Yettel’s orbit if under written permission of the

data/tool Owner is available. Appropriate protection mechanism must be applied for these devices or information resources as well.

If there is a valid business need for using removable media (e.g., pendrive) it must be used with password protection. Any Yettel business data must be deleted from the removable media using industry best practice secure deletion method after it is not needed anymore.

Yettel may make a copy of the encryption key and store it and may use them to reverse business information.

3.4 External Data transfer

Data transfer between Yettel and third party must be done in a secure way. This including but not limited to the following:

- Attachment sent by email must encrypted (using 7-Zip encryption or similar method). The password must be complex (at least 8 character, upper and lower case)
- Secure data transfer tools can be used, but only after the written approval of Information Security Office
- It is the Contracted Partner's responsibility to protect Yettel business information

3.5 VPN

As a baseline Contracted Partners cannot have VPN access. If VPN access is needed it must be part of the contract. If the contract does not contain it then it needs to be approved by the relevant Business Director and Procurement Director.

4 Access protection

4.1 Regulations for access data

Access authorizations are used for the protection of information systems of Yettel, including but not limited to infrastructure, information resources and data.

User data for access, such as PIN, passwords, certifications, tokens, ID Cards and intelligent cards may only be used by their holders. Access data shall be memorized or stored in safe place. Access data shall not be forwarded, shared, published or made public for people or organizations who are not liable for these data.

If the confidentiality of data providing access is compromised (known or lost to others), such data shall be disabled immediately and, in any case, new ones shall be chosen instead. In the event of a suspicion of misuse of access data, this shall be reported to the *Information Security Office* immediately (see contact information in *Appendix I*).

All the Contracted Partners who have access to Yettel's information assets are individually liable to know and comply with the applicable regulations on access protection and the use of access data.

A person whose access data provides access to any resource may be held liable for all actions taken with their access data.

The screen of different devices, such as computers or phones, shall be closed when the user cannot control them (for example, computers shall be locked (Windows+L) before leaving the desk and locking the mobile phones with PIN protection).

4.2 Regulations for ID Cards

Yettel might provide temporary ID Cards for Contracted Partners who are working together with Yettel on a long term. Otherwise, visitor Card is provided.

Any person who has a visitor, temporary or permanent ID Card provided by Yettel, including Contracted Parties or other authorized personnel, shall visibly wear his identification card at Yettel's premises.

The ID Card and mobile phone with the access identification feature are strictly personal and identify only the person who received it. It is strictly forbidden to give the ID Card and the mobile phone with the access identification capability to another person. This applies for the colleagues of the Third Party as well.

If an unauthorized person enters Yettel's territory because of a deliberate or gross negligence on the part of a user, this may entail penalties for employment. In the event of the loss of or theft of the identification card and the identification of a mobile phone assigned to it, an immediate notification shall be made. (For contact information, see *Appendix II*.)

People with a temporary (visitor) ID card shall be accompanied by a Yettel employee with permanent access right for the entire duration of their stay.

Everyone is obliged to notify the *Physical Security Manager* immediately of any abnormalities related to the access control system. (For contact information, see *Appendix II*.)

In case of loss or theft of the visitor/temporary ID Card, it shall be immediately reported to Physical Security Manager.

Temporary and permanent ID Cards needs to be handed back up on leaving or at the end of the long-term working relationship.

5 Regulations for electronic messaging

In certain cases, Contracted Partners can have Yettel email addresses. These cases are typically are the following:

In case of a Contracted Partner has Yettel email address the following applies:

- Electronic messaging should be used primary for business purposes. Public email accounts are (e.g., Gmail) forbidden for business purposes.
- Private usage is acceptable but must be kept on a minimum. Users must have a dedicated folder clearly indicated to be private (like named „Private" or „Personal") for these emails.
- Must not forward spams, email chains, offensive or unsolicited emails
- Signature must be part of the business emails. Private emails shall not contain text that may be related to Yettel or that gives the impression that the person mediates the opinion of Yettel.
- The content of the email must be compliant with Yettel's Code of ethics and applicable regulations Specially, but not limited to: pornographic, offensive, racist and other discriminative materials.
- The Contracted Partner must make sure only the appropriate personal receives the emails. It is always recommended to double check the "to" and "cc" lines.
- It is recommended to set up "out of office" automated reply in case of annual leave, sick leave etc.

As part of Security governance regime Yettel has the mandate for implementing the following security measures:

- Yettel may check the contents of emails for compliance or for security reasons and this is also accepted by third-party users for emails sent to Yettel. (This is also listed on Yettel's website.)
- Yettel has the right to place a disclaimer or other legal statement to the end of outgoing messages sent to external addresses.

6 Regulations for internet use

In Yettel Headquarters, Contracted Partners must use Guest Wifi only. Contracted parties not allowed to use the internet via Yettel networks cable.

During the usage of the internet, Contract Partners must comply with the following:

- Comply with Code of Conduct and regulatory requirements
- It is specially forbidden to use the internet access for pornographic, offensive, racist or gambling purposes.
- Connecting to and using peer-to-peer file exchange networks are strictly prohibited.
- It is strictly forbidden to use Yettel's internet access for attacking others or to commit actions explicitly prohibited by law.
- It is not allowed to download not authorized software's from the Internet.

7 Regulations for mobile devices and IT resources

In some cases, Contracted Partners can have Yettel provided mobile devices and IT resource. In those cases, the Contracted Partners must comply with *Local Manual – Information Security Regulations for Users* and *Local Manual – Rules of Mobile Devices and Remote Working*.

Otherwise, it is the responsibility of Contracted Partners to use protected and secure device. If Contracted Partners use their device (which is not under Yettel's orbit) the following must be followed:

- the device must be hardware encrypted if it is technically possible
- the device must be password protected
- the device must be virus protected

8 Regulation for breach of rules

Failure to comply with these Terms may, inter alia, entail the following sanctions:

- Verbal warning
- Written warning
- termination of the Contract
- other sanctions resulting from a labour contract or legislation.

Members of the staff concerned may also be subject to financial / material compensation obligation.

All individuals required to comply with these requirements are obliged to know and comply at all times with these and other regulations regarding Yettel's information assets in Hungary.

9 Definitions

Authorized personnel

Authorized personnel to have access to certain information and / or IT resources. Eligibility is ensured by a documented procedure. Personnel who have licensing powers in certain areas, such as access rights, modifications, enhancements, purchases, software packages, use of tools, etc., may also be qualified personnel. respect.

Licensed software

A software authorized by the authorized personnel of Yettel or Information Security for which Yettel has a valid license.

Mobile device

Any managed device that can be used outside Yettel's on-premise environment, including

"handheld" devices, mobile phones, laptops, tablets, etc.

Information device

Information systems include all software and hardware together with data stored there, including fixed and portable IT equipment, handheld devices, information systems, networks and any other IT infrastructure or service that can be used to store, process and create data or treatment.

IT resources

IT resources include all software and hardware resources, including stationary and portable IT equipment, "handheld" devices, information systems, networks and any other IT infrastructure or service that can store, process, create, or manage data serve.

Premises of Yettel

For the purposes of this document, Yettel's premises are all buildings, premises, premises and areas owned or controlled by Yettel.

Owner

It is an individual or organizational unit who has a comprehensive liability for a system, process or information. In this context, "liable" does not refer to the person who actually owns the asset or resource of the asset.

Private information

Personal data of employees, such as personal photos, video and sound recordings, documents, emails, etc., which may not contain any personal information that may be related to the professional activity of Yettel in Hungary or whose license or copyright and / employee.

Malicious program

Malicious software that is used to destroy and / or leak data. Malicious programs include viruses, worms, keyboard logging applications, and so on.

Electronic message

Electronic messages include, but not limited to, emails sent over the internet or locally, SMS (short message), MMS (multimedia message), EDI (electronic data interchange) and instant messaging (e.g., Skype).

Electronic messaging services

Services used for electronic messaging.

Data medium

Any device or device component, such as CD, DVD, portable or fixed hard disk, SIM card, and other similar or similar features, or any device that has an integral part of it for the same or similar purpose such as PDA, mobile phone, and so on.

Files for entertainment

Files that contain non-business information, such as entertaining music, video, pictures, or text files.

Spam

Unwanted mail sent in bulk.

Executable software module

A program object (ActiveX control, Java applet, Explorer extension, etc.) that can be downloaded and run with a compatible browser. Malicious Executable Software Modules can perform any operation that may result in damage or damage to software or data on your computer.

Internet

A global network of connected networks that provides services and information with the standard Internet Protocol Kit.

Peer-to-peer (P2P)

An application layer virtual computer network, where all computers work simultaneously as clients and servers serving other computers.

USER

A user is a person who utilizes a computer or network service inside Yettel premises or technical infrastructure.

CONTRACTOR

A contractor is a person or company that does work for Yettel and has access to data, information systems and/or network services.

Yettel

Yettel refers to Yettel Magyarország Zrt.

CETIN

CETIN refers to CETIN Hungary Zrt.

10 Appendix

10.1 Appendix 1

Information security in each country:

- Yettel Magyarország Zrt.: information.security.thu@yettel.hu
- CETIN Hungary Zrt.: soc@cetin.hu

10.2 Appendix 2

Notification addresses, phone numbers for theft or loss of information or identity cards:

- Yettel Magyarország Zrt.: karokozas@yettel.hu, +36204447510