# Guidelines on Information Security Principles for Third Parties and Guidelines for Authorized Persons

**Summary:** This document defines the basic security requirements for a third party*, which with regard to a business relationship with the company Orange Slovensko, a.s. (hereinafter only “Orange”) must have access to the physical premises of the company Orange and/or to computer systems and networks (hereinafter “information systems”) in the environment** of the company Orange. The goal is to minimize security risks associated with the operation of a third party in the environment of the company Orange and pass to it the responsibility for possible consequences of non-compliance with these security requirements.
The third party undertakes to comply with these requirements

* For the purpose of this document a third party shall mean the Supplier in accordance with the General Purchase Terms of company Orange.

** For the purposes of this document the environment of the company Orange shall mean the physical and logical premises, over which the company Orange has a full control, i.e. it either directly owns them or leases them.



Orange Slovensko, a.s.
Metodova 8, 821 08 Bratislava

**Content:**






Orange Slovensko, a.s.
Metodova 8, 821 08 Bratislava

## 1.0 Introduction

The purpose of the instruction is to inform the third party about security requirements, on the basis of which the third party by its signature declares its consent and willingness to meet these requirements. By its signature in the declaration of a third party the third party undertakes to comply with these requirements. A template of the declaration is enclosed at the end of this document (see Appendix A). These principles apply to any third party which has a contractual relationship with the company Orange, on the basis of which it becomes a part of the internal environment of the company during the period necessary for the execution of the agreed works or project.

### 1.1 Applicability

The following table defines a list of chapters that are subject of the instruction of a third party related to the persons of third parties, depending on their access and job descriptions in the company Orange.

| **Type of access to the company Orange** | **Compulsory chapters** (including all sub-chapters) | **Note** |
|---|---|---|
| Persons with **ONLY** physical access to the environment of the company Orange | Chap. 2; 4 to 7 | In case that the person is a processor as defined by applicable legal regulations for the protection of personal data he/she has to be instructed also pursuant to Appendix B. |
| Persons with logical access to the environment of the company Orange | Chap. 3 to 7 | In case that the person is a processor as defined by applicable legal regulations for the protection of personal data he/she has to be instructed also pursuant to Amendment B. |
| Persons with physical and logical access to the environment of the company Orange | All chapters of this procedure | In case that the person is a processor as defined by applicable legal regulations for the protection of personal data he/she has to be instructed also pursuant to Amendment B. |

## 2.0 Physical security

### 2.1 Basic principles of physical security

Physical premises covered by the rules referred to in this document, shall mean administrative and technological premises including accessories (kitchens, hallways, restrooms, showers, warehouses, etc.) used by the company Orange temporarily or permanently for the performance of its business activities. These are also the areas in which the company Orange conducts an electronic or physical control of access or movement in these areas. This definition does not apply to premises permanently open to the public without any access control.
The general rule is that the entry of each person to the premises of the company Orange is controlled. Any person of a third party may enter only into those areas for which it has acquired a permission to enter.
The entry and movement of authorized third-party persons must be limited only to the time necessary to carry out the activities of that person who has been entrusted with them.
In addition to usual personal items only such things can be brought into the premises of the company Orange which are necessary for the performance of the activities of the third party. In particular, it is forbidden to bring personal computers, electronic information storage devices and electronic information carriers (e.g. notebooks, USB drives, portable hard drives, portable burners, etc.) to the premises of the company Orange unless these devices serve exclusively for the performance of the third-party activities

in the premises of the company Orange.
It is strictly forbidden to bring out of the premises of the company Orange any technical equipment, computers, information carriers, documents and other things belonging to the company Orange unless it is necessary for the performance of the third-party activities in accordance with the relevant contract.
This document does not regulate the safety and health protection at work and the fire protection within the premises of the company Orange.

## 2.2 Control of entry

Only an authorized person of a third party may enter the premises of the company Orange:

- equipped with an access card and an identification card of the company Orange issued on his/her name, or
- accompanied by an employee of the company Orange.

The basic access control is performed through the Electronic Access Control system (VS) based on the allocation and use of non-contact access cards. Exceptionally, for premises where the electronic access control system is not installed, the control is done by controlling the allocation and use of mechanical keys.

### 2.2.1 Permit to enter

In general, the principle is that the entry of any person representing a third party must be permitted. Authorized third-party persons are only allowed to enter those premises that are necessarily related to the performance of the person's activities. The permission to enter the company Orange premises (except within the visitor mode) is conditioned at least by:

- the existence of a legal relationship between the third party and the company Orange,
- a declaration of the requesting person of the third party that he or she has been informed about the rules set out in this document or in the Third-Party Security Policy of the company Orange and that he/she undertakes to abide by them,
- a declaration on the instruction about the protection of personal data that may be located in the premises or in the information systems of the company Orange (see Appendix B).

A permit to enter in the form of allocation of an access card is granted on the name of a particular person. A permit to enter for an authorized person of a third party is arranged by an employee of the company Orange responsible for the activities of the third party by a prescribed procedure at the Orange CorpSec department.

### 2.2.2 Rules of entry and use of access cards

The access card is non-transferable and entitles only the person on whose name it was issued for the entry. The use of an access card or identification card by another person or its lending (handing over, disclosure) to another person is strictly prohibited.

The cardholder is authorized to use it only to enter the premises where the entry is allowed for him/her. If the room into which the authorized person enters is secured by a VS reading device, the use of the access card is always mandatory, even if the door to the room is open (e.g. by another entering person). It is also necessary to use the access card always at the main entrance to the premises of the company Orange (e.g. turnstiles at the main entrance), and that also in the case when a person enters for example when bringing in material through a special uncontrolled entry (cargo doors, gates, ramps, etc.). Upon entering the premises outside normal office hours, the security service may require a separate registration in the guestbook even if the person is allowed to enter the premises of the company Orange on the basis of the assigned access card.

The cardholder is also obliged to protect the access card from damage, destruction or loss.

In the event of theft or loss of the access card, the holder is obliged to immediately report this fact to the competent officer of the company Orange responsible for the activity of the third party, to Human Resource (HR) section personnel or to the company Orange CorpSec (phone No. 0908 004 112, e-mail: xsm_admin@orange.sk).

In addition to the access cards authorized persons of a third party having their permanent place of work in the premises of the company Orange must also use ID cards of the company Orange with a colour photo, logo of the company Orange, their name, position and the firm they represent.

THE PERSON TO WHOM THE CARD WAS ALLOCATED IS ALWAYS RESPONSIBLE FOR THE USE OF THE CARD, BUT ALSO FOR ITS POSSIBLE ABUSE!!!

#### 2.2.3 Mode of allocation and use of mechanical keys

Mechanical keys can be allocated only if the entry to the premises where the authorized person of a third party is to operate according to the relevant contract, is not possible only using an access card, or if the premises are not controlled by an electronic SV.

If it is an area that is controlled by SV and at the same time it is necessary to use a mechanical key the authorized person is obliged to use the mechanical key and the access card always simultaneously, i.e. it is not permitted to use only the key without placing the access card on the SV reading device.

USE OF THE SO-CALLED PASSKEY IS PROHIBITED!!!

The permission to enter the premises which are accessible through the use of a mechanical key, assigning of the keys and their use is governed by special rules laid down by the Facility Department of the Human Resources section or the rules set out in the relevant contract with the third party.

If such rules have not been issued, or the third party has not undertaken to observe such rule the allocation and use of mechanical keys is governed by the provisions of paragraph 2.2 of this document, with the exception that any damage, destruction or loss of a mechanical key is promptly reported to the relevant responsible employee of the company Orange, who is responsible for the activities of the third party or to the personnel of the human resources (HR) section.

### 2.3 Premises with a special regime

The entry into the premises which, according to the internal security procedures (top management offices, premises of the company Orange CorpSec, s.r.o., warehouses of goods and material, cash desks, selected meeting rooms, technological rooms, etc.), are to be specially protected, is subject to the permission of the director of the relevant section of the company Orange. Authorized persons of third parties may enter and move in these premises only in the presence of an authorized employee of the company Orange unless otherwise agreed in the contract with the third party or the appropriate entry permit.
If third parties are allowed to enter the premises of the company Orange monitored by the Intrusion Alarm System (IAS), they can enter these premises only if they have been granted a unique access code to the IAS.

## 3.0 Logical security

The logical environment to which the rules set out in this document apply, shall mean the information systems in the environment of the company Orange temporarily or permanently used by the company Orange to carry out its business activities.

It is generally applied to the logical environment, that the access of third parties to the information systems of the company Orange is managed and implemented solely through the Identity Access Management (IAM). Another way of granting access is not possible. The access to information systems for third-party employees is managed solely by internal employees responsible for the third party. Any third-party person can only access those information systems for which it has obtained an authorization through the IAM.

### 3.1 Use of personal computers

Computers and computing resources can be used only for a service or commercial purpose determined in advance. In the event of doubts about the purpose, a reference to the specific contract or agreement on the purpose of the third-party presence in the company Orange will be used. The use

of such devices for private purposes is prohibited.

## 3.2 Use of personal computers belonging to the company Orange

If a third-party employee is allowed to use a personal computer or computing device belonging to the company Orange, he may not in particular:

- move it (unless it is a portable device such as a tablet, a laptop, and it is necessary for the performance of the contract);
- open it, disassemble
- connect or disconnect its peripherals,
- install any software on it including drivers for hardware or software etc.
- if the computer is connected to the local computer network of the company Orange he must not create additional, uncontrolled connections to other computers and systems (mainly to the Internet) e.g. via wireless LAN (Wi-Fi), GPRS, etc. This issue is solved in the company Orange exclusively by the authorized IT staff (HelpDesk).

Additional rules for third parties and their employees related to the use of personal computers belonging to the company Orange are defined in the following chapters.

### 3.2.1 Access to the local computer network

If a third party gets an access to the local computer network in the company Orange:

- it must have its network (Windows domain) accounts named according to the surname of the user and an attribute designating the third party (an extern, see the section on using e-mail below); such an account must never get the privilege of a local administrator in a way other than by a controlled process
- it must not provide its account authentication data to another person - the user of the account is in any case responsible for the use of the assigned account,
- the person must protect the access to his/ her computer if not in use,
- he/she must not use locally shared folders (Windows shares) to exchange data among other users (typically a file server managed by a trusted party, such as HelpDesk or a domain administrator is usually assigned for such purpose).

### 3.2.2 Internet access

If a third-party employee was authorized to use the Internet access from the local network of the company Orange, he must not:

- access sites with anarchist, terrorist or pornographic content, including sites containing illegal software and hacking sites,
- download excessive data volumes unless they have any connection with the needs of the company Orange or the purpose of the third party stay in the company Orange,
- download software for personal, non-business use,
- use the Internet for private or other commercial purposes,
- use the Internet connections for social networks, chat groups/services, for the use of webmail services, to send and download files from public or private web-sharing servers, or to exchange files via p2p networks and the like, especially if they are not related to the purpose of the stay of the third party in the company Orange,
- attempt to gain unauthorized access to remote computer systems or files on the Internet or intranet,
- violate the privacy of other Internet users (spam, social engineering, etc.)
- access the Internet directly from the so-called "production" systems,

- create HTTP tunnels (e.g. encapsulate other protocols within HTTP) into public (Internet) resources.

#### 3.2.3 Use of e-mail

If a third-party employee was authorized to use the e-mail from the local network of the company Orange, he must not:

- act or sign as an employee of the company Orange and in his e-mail address (SMTP) including the displayed name and the alias he must have the identification of an extern (ext, x _, e.g. ext_name.surname@orange.sk)

and also, must not use the e-mail for:

- any purpose that could constitute a violation of applicable laws of the Slovak Republic,
- private or other commercial activities that have no relation to the commercial interests of the company Orange,
- sending spam with attachments (pictures, presentations, executables, etc.). Sending an e-mail is subject to internal rules and restrictions of the company Orange,
- the proliferation of private opinions, "chain letters", or inappropriate messages to distribution lists of addressees or to individuals (such as requests for expression of political opinions, requests for donations, etc.),
- other conduct that is contrary to good morals, and may have a direct or indirect impact on the reputation or business activities of the company Orange.

#### 3.2.4 Copyrights and software licenses

With the exception of service and other contractual relationships that define it in advance third-party employees must not install any unauthorized software on PCs of the company Orange. For each software that is to be used, there must be a corresponding license, which is the responsibility of the Orange Slovensko HelpDesk.

#### 3.2.5 Rules for antivirus protection

Personal computers must always have an antivirus software installed with up-to-date definition files. It is the standard responsibility of the HelpDesk. The user of a computer must not in any way restrict the functionality of the antivirus software and if he himself detects that his computer has no antivirus protection or is without the latest antivirus definition file, he is obliged to immediately inform the Helpdesk about this situation.

### 3.3 Use of personal computers belonging to a third party

Computers not belonging to the company Orange must not be connected to the local computer network of the company Orange and they must not have access to the Internet, only provided that the third party has been granted an exemption (see chapter 5).

Employees of third parties must not install or use their own communications equipment in the company Orange or use them for an uncontrolled access to the Internet and sharing of information (e.g. modems, faxes, or wi-fi devices).

If a third party is allowed to use their own computers in the local computer network of the company Orange, it must meet the requirements specified in Chapter 3.2, except for the parts on the use of software (chapter 3.2.4) and on viruses (3.2.5), to which special provisions defined in the following chapters are applied.

#### 3.3.1 Rules for the use of software

If the third-party PCs are a part of the local computer network of the company Orange, the third party must not use the software or hardware, which can be misused against the company Orange. These include network sniffers, analyzers of network traffic, virus toolkits, port scanners, scanners of shared network resources, etc.

At the same time, it is assumed that each software installed on those computers is properly licensed, for which the third party is responsible, regardless of licensing rules and contractual obligations of the company Orange.

### 3.3.2 Rules for antivirus protection

If the third party is allowed to use their own computers in the company Orange it is obliged to use properly updated antivirus software on them and is responsible for possible consequences for the company Orange in the case of a virus problem caused by the operation of the third party in the company Orange.

## 4.0 Protection of assets and information

In the premises of the company Orange third parties are prohibited:

- to bring out and move any things belonging to the company Orange or its employees, in particular computers, computing devices, other technologies etc.
- to switch on, switch off or otherwise manipulate with the technical devices placed in the premises of the company Orange,

if these activities are not a part of the performance of the third party based on the relevant contract with the company Orange.

It is also prohibited:

- to bring personal computers, electronic information storage devices and electronic information carriers (e.g. notebooks, USB drives, portable hard disks, portable burners, etc.) to the premises of the company Orange unless these devices serve exclusively for the performance of the third-party activities in the premises of the company Orange,
- to bring out from the premises of the company Orange any electronic information carriers, computers and documents belonging to the company Orange and in any other way to handle these things, unless it is expressly a part of the performance of the third party in accordance with the relevant contract.

The third-party employees who in the provision of their services come into contact with a service/ business information or personal data belonging to the company Orange, must not use, misuse, disclose or provide this information without an authorization to any other parties.

Since the company Orange in connection with the performance of their business activities processes personal data in its information system, any authorized person of a third party who is to be allowed to enter the premises and/or environment of the company Orange, is obliged to sign an instruction on their responsibilities for the case he/she comes into contact with personal data, to the extent specified in Appendix B hereto.

The third parties acknowledge that for the purposes of protection of the assets some of the premises of the company Orange are monitored by the closed-circuit television system (CCTV) or Intrusion Alarm System (IAS).

## 5.0 Applications, procedures and management of exemptions

All applications for third-party authorized persons for an access, allocation of resources, assignment of privileges, etc. that are necessary for the performance of the third-party activities in the company Orange are filed on appropriate forms (QAF) or through applications serving for that purposes (e.g. IAM), and in accordance with applicable internal procedures applicable in the company Orange to third parties.
If such applications and procedures are not formalized in the company Orange and are related to the rules specified in this policy, or if it is the case of any of the exemptions from the requirements mentioned in this document, they are addressed individually through the Security Manager of the company Orange. In order to obtain a consent to an unformalized application or to granting an exemption, it is usually necessary to provide a detailed justification. An application for an exemption is filed through the appropriate manager of the company Orange who coordinates the third-party activity in the company Orange.

The relevant extract from the written contract between the company Orange and the third party is considered to be the best argument for obtaining an exemption from these security rules for third parties.

## 6.0 Non-compliance with the rules

Non-compliance with the requirements referred to in this document is considered to be a security incident that escalates on the managerial level in the company of Orange, as well as with a third party, which may ultimately lead to contractual penalties or claims for damages against the third party, or to a termination of the contractual relationship with the third party on the basis of the relevant provisions of the contract.

## 7.0 Responsibility for reporting security incidents

Third-party personnel is responsible for reporting security incidents, which they are aware of in the exercise of their activities in the company Orange or which they directly witness.
A security incident is considered to be such an event that shows signs of a criminal activity and/or it is such a violation of security rules of the company Orange (at minimum as defined by this document), which can have an impact on business and business interests of the company Orange, on its legal obligations, or lead to a negative publicity.
The events that will be automatically considered to be a security incident include, inter alia:

- freely accessible (non-secured) personal data or data representing a telecommunications secret of the customers and personal data of the employees of the company Orange, whether in a paper or electronic form
- disclosure of trade secrets or classified information of the company Orange
- impersonating another person, in order to get a physical/logical access or permission to enter the premises of the company Orange, or its resources
- unauthorized access to physical and logical premises of the company Orange
- a theft of physical property or intellectual property of the company Orange
- providing kickbacks in exchange for benefits
- threat of injury to a person, his/her life or property.

A security incident must be reported in a timely manner and with appropriate accuracy at the appropriate management level of the company Orange and the company Orange CorpSec, s.r.o.

## Appendix A

## TEMPLATE

## Declaration on the instruction of an authorized person (staff member) of a third party on the security rules in the company Orange

The undersigned employee/associate of the third party:

Name and surname: .....
Position: .....
Name of the third party: .....
Reg. No.: .....

Hereby I declare that I have been advised of the security rules and policy of the company Orange Slovensko, a.s. specified in the document: “Physical security rules for the entry of third parties into the premises of the company Orange Slovensko, a.s.” which is a part of the Contract for ....., concluded between the company Orange Slovensko, a.s. and the third party on..... .

I also declare that I have understood the security rules and policy and undertake to observe them in their full scope in carrying out my activities in/for the company Orange Slovensko, a.s.

In Bratislava, dated.....

.....
Name and surname
Position

## Appendix B

## TEMPLATE

### Instruction of the person who may have access to personal data

processed in information systems of the company Orange Slovensko, a.s.

*(Note: this instruction applies to the suppliers, their employees, or other persons who are authorized to enter the facilities, premises of the company Orange Slovensko, a.s., or who carry out maintenance, repair, support, or other activities on information systems of the company Orange Slovensko, a.s.)*

*Name: .....*

*Position: .....*

*(hereinafter only "the informed person")*

Employee of the company/supplier:

*Business name: .....*

*Registered office/Place of business: .....*

*Reg. No.: ....., VAT ID No.: .....*

*Contract/Order: ....., dated .....*

*(hereinafter only "the Partner")*

I hereby confirm that as a person authorized to enter the facilities and premises of the company Orange Slovensko, a.s., or performing maintenance, repair, support or other activities on the information systems of the company Orange Slovensko, a.s. I have been informed about the following rights and obligations arising from the applicable legislation governing the protection of personal data, e.g. the Regulation of the European Parliament and of the Council (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC; valid Slovak law on the protection of personal data; the implementing rules for the said legislation, etc. (hereinafter referred to as "**applicable laws on the protection of personal data**"), and on the responsibility for their violation;

1. The informed person is not authorized to process, remove, copy, acquaint oneself with, or otherwise dispose of the personal data of the subscribers of the public communications services of the company Orange Slovensko, a.s., or with the personal data of the employees of the company Orange Slovensko, a.s., or other data subjects collected in the information systems or in the premises of the company Orange Slovensko, a.s.
2. If after entering the facilities and premises of the company Orange Slovensko, a.s. or in the performance of maintenance, repair, support or other activities on information systems of the company Orange Slovensko, a.s. the informed person comes into contact with personal data, he/she shall forthwith in any form inform the responsible employee of the company Orange Slovensko, a.s. about it
3. If after entering the facilities and premises of the company Orange Slovensko, a.s. or in the performance of maintenance, repair, support or other activities on information systems of the company Orange Slovensko, a.s. the informed person acquires personal information, it is obliged immediately to hand over the personal data or the carrier, on which they are stored, or recorded (including the paper), to the responsible employee of the company Orange Slovensko, a.s. Such a person shall not, in any case, copy the carrier or make any reproduction of it.

4. The informed person may enter into the information systems of the company Orange Slovensko, a.s., only to the extent necessary and only if it is related to the legitimate performance of its activities, and that after a prior notification of the responsible employee of the company Orange Slovensko, a.s.
5. The informed person must not interfere in any way with the information system of the company Orange Slovensko, a.s., which may result in its deterioration, damage, failure, destruction, or any disablement. If the informed person in accordance with his/her authorizations for any activities on information systems of the company Orange Slovensko, a.s. is to take a certain action, where, taking into account the reasonable professional care, it can be assumed that such intervention can have the above described impact on the information system of the company Orange Slovensko, a.s., he/she is obliged to notify in advance a responsible employee of the company Orange Slovensko, a.s.
6. The informed person is obliged to keep confidential all personal data with which he/she came into contact in the performance of his/her activities, as well as the manner and the extent of their processing in the information systems of the company Orange Slovensko, a.s. In particular, the informed person is obliged not to use the personal data with which he/she comes into contact for personal use and must not disclose them and provide them to a third party or make them public. The informed person shall maintain the confidentiality obligation under this section even after the termination of his/her activities for the company Orange Slovensko, a.s.
7. In the execution of his/her activities the informed person shall comply solely with the relevant applicable legislation on personal data protection, the agreement concluded between him/her or his/her employer/contractual partner and the company Orange Slovensko, a.s. this Instruction and the guidelines of the company Orange Slovensko, a.s., otherwise the informed person is fully responsible for a violation of these obligations.

At the same time as an informed person I declare that I understand my rights and obligations about which I was informed and undertake to comply with them.

In ....., dated .....

.....
Legible name and signature of the informed person

The instruction was carried out for the partner by:

Name: ....., section: .....

Tel.: ....., fax: ....., e-mail: .....

.....
Signature



Orange Slovensko, a.s.
Metodova 8, 821 08 Bratislava