2024 - ISMS.IT.I.03[EN] Corporate IT-services users work regulation

Document reference

INFORMATION SECURITY MANAGEMENT SYSTEM	
Instruction	
Ref:	ISMS.IT.I.03[EN]
Title:	Corporate IT-services users work regulation
Version:	1.0

Revision history

Date	Version	Author	Change details
12.04.2023	1.0	Vladislav Nikitin	Document reference was added.

Table of Contents

1. Introduction

1.1. Field of application

The Document is necessary for application by all structural departments of the Company Group "Itransition" (hereinafter the Company).

1.2. Aim of the document

The present Regulation is developed for updating requirements, which were in effect earlier as the "Rules of working in the corporate network and the Company equipment maintenance manual" of 10.04.2012, in accordance with international standards ISO 27001, ISO 9001, and the GDPR of 2018.

The Regulation determines general working terms of all corporate IT-services users' categories: full-time/part-time staff, staff undergoing studying and internship, persons temporarily staying in the Company office (clients, partners, and subcontractors, hereinafter Guests).

Thorough rules of working with information systems, services and other Company resources are determined in accordance with the provided IT-services Instructions and Manuals, and SLAs (Service Level Agreements).

Compliance with the present Regulation requirements is necessary for all of the Company staff; it provides equipment maintenance cost reduction, addresses information services malfunctions, and minimises information security threats to the Company resources. Responsibility for informing about and abiding by the present Rules by Guests lies with the Company staff, who provide Guests' reception and escort during their time in the Company Office, and on the staff, by the initiative of which the access to the Company group resources or IT-services was presented.

1.3. General provisions

The Company has the Information Security Management System (ISMS) in effect, which is subject to continuous review and improvement.

The requirements of the present Regulation are based on and complement requirements, stated in the ISMS documents, including its privacy policies (ISMS.IT.PP).

All Company group users' categories must undergo an information security briefing in accordance with the procedure, described in the ISMS.IT.I.01 Information security briefing procedure.

All identified security incidents must be registered in accordance with the ISMS.IT.I.02 Information security violationreporting procedure.

2. Access to corporate network resources

The Company provides all staff members with access to the resources of the corporate network, information systems, services and other resources of the Company in the amount necessary to fulfil their respective duties and tasks. The Head of the Department, in which the employee works, determines Job descriptions, tasks, responsibilities and level of access to the Company's resources.

Access to the corporate network resources, information systems, services and other Company resources may be presented to other users' categories of the Company group, including Guests, on a declarative basis through the users' requests registration system (HelpDesk). The request should be on behalf of the project manager or the user's mentor, and with the mandatory confirmation of a responsible person (technical coordinator), indicating the resource name, usage/access purposes, and necessary duration.

To control and separate users' authorities in the Company, the Active Directory (AD) service is used. Identification and authentication of users in the Company's information systems is carried out using an AD account consisting of a unique login name and password.

Note: The username (login) consists of the Latin character of the first letter of the real and full username, the period character "." and then transliteration of the Russian variant of writing the user's last name in Latin. For a unified transformation of the name and last name, a single script program is used, located at https://jira.itransition.com/translate.html.

User password requirements are defined in the ISMS.IT.PP.02 Password Policy. This policy also defines the requirements for the procedure for changing and recovering user passwords. The fact of a user account lockdown is a security incident, which is subject to registration, accounting, and analysis.

2.1. Access provision order

An AD account for a new employee is created by the MDIS users support service (hereinafter ServiceDesk) in accordance with a standard form application in the HelpDesk system from the HR department. Applications are processed in the admission order within 1 working day.

Temporary Guest AD-account creation is performed by the ServiceDesk in accordance with a standard form application from a project manager, coordinator, or the head of the structural unit, to which a Guest has arrived.

Application forms for creating AD accounts for new employees or Guests are presented in "Processing applications system for new employees' registration" and "AD guest account creation" documents.

For the project needs at the request of authorised officials (project managers, technical coordinators), in the corporate AD or corporate systems (Jira, Wiki, etc.), so-called project /service accounts can be created. The access rights of such accounts are limited to the minimum, required to complete the project task. Use of such accounts for tasks, other than declared for the project, is prohibited. The storage and use of passwords for project/service accounts are subject to the same restrictions as for the storage and use of passwords for user AD accounts.

2.2. Access suspend order

An AD account for a new employee automatically goes to the "suspended" state after the time specified in the application for its creation (usually equal to the probation period of the new employee). To resume the AD account effect, a standard form application for the probation period extension, or an employee transfer to a full-time (permanent) staff status, is needed from an HR employee, to whom the new employees' mentor provides necessary information. Such an application, in order to avoid the forced standstill of a new employee, can be sent by his/her mentor before the end of the trial period.

If there is a need to suspend the operation of an AD account, including if it is compromised, its owner (user) or the head of the structural unit (PM, RM, TC, DM) creates a request to the ServiceDesk.

If abnormal activity is detected on the part of the user equipment, violations of these rules or events that threaten the health and/or security of the Company's systems are detected, MDIS may immediately suspend the AD account or take other technical measures, while informing the head of the relevant Department about the revealed fact.

2.3. Access termination order

Access termination to the Company's resources is performed in accordance with a standard form application under the procedure, described in the "AD account blocking information" document.

3. Equipment usage order

The Company provides all staff members with temporary equipment for resolving specified tasks and the performance of their duties. This equipment is subject to return upon the dismissal of the employee from the Company. The employee of the Company bears material responsibility for the equipment issued to him. The employee must preserve corporate equipment, including workplace and peripheral devices, as well as equipment in common areas (meeting rooms, training classes, game rooms, kitchens, corridors, and other specialised premises), prevent actions directed to damage the Company's property, and to inform of any reported damage in a timely manner. When being returned to the warehouse, the equipment must be clean, without any changes in its appearance (drawings, airbrushing, stickers, and their traces - glue residues, scraps, foreign bodies, etc.)

If the user detects or makes any mechanical or other damage to their equipment or the Company's property, including shared equipment (shared printers, conference room equipment, meeting rooms, etc.), the user must immediately register the application in the HelpDesk system. In the absence of such an opportunity, the employee is required to inform the project manager, technical coordinator, and the service group it.store@itransition.com by e-mail.

3.1. Equipment provision

Typical equipment (personal computer, monitor, keyboard, and mouse) is provided to a new employee based on an application from the Office Service employees to ServiceDesk. The application form is defined in the "Processing applications system for new employees' registration" document.

Additional equipment (for example, telephone, headphones) is provided on the basis of the user's application to ServiceDesk in agreement with his PM or RM; non-standard equipment is provided on the basis of the application of the head of the structural unit, in agreement with the head of the relevant Department, or a person authorised by him.

Specific equipment necessary for carrying out works related to the project activity is acquired by the department independently. Its connection to equipment and corporate systems is carried out in consultation with the competent staff of MDIS. The responsibility for possible security incidents for self-connecting non-typical equipment is borne by the employees who carried out these actions.

3.2. Equipment replacement

Equipment replacement is carried out in the following cases:

1. Fatal malfunctions, maintained equipment failures occurrences;
2. Equipment established lifetime expiration;
3. An occurrence of a justified production need for replacement;

Replacement of equipment is performed in a planned manner, according to the order of applications submitted by the responsible officials of the departments (included in the AD groups Workstation.Managers or Workstation.Assistant.Managers) to the equipment updates requests portal. Applications are reviewed monthly in a planned manner. In an emergency, they can be considered unscheduled, upon the application of the responsible persons.

3.3. Equipment return order

In case of dismissal, employees must present equipment assigned to them to the MDIS employee, by tentatively creating a request at the ServiceDesk, with the coordination of a transfer place and time. Equipment must be presented in a working condition and completeness, according to the configuration issued.

3.4. Personal equipment usage

Basic principles and requirements for the use of personal equipment are described in ISMS.IT.PP.05. BYOD (Bring Your Own Devices) policy. The Company staff has the opportunity to use personal equipment (display, workstation, laptop) as a working one, having previously agreed on this with the head of their department, and having approved their model used at the IT department (an approval request must be sent to HelpDesk). The software installed on the workstation (laptop) must comply with the policies adopted by the Company.

The current version of the supported and authorised software Listis placed in the Confluence corporate system.

Computer equipment (including personal equipment, used for working purposes and on the conditions set forth above), equipment, supplies, corporate network resources, and other Company services must be used for official (productive) purposes. The fulfilment of other tasks and use of the equipment, and resources for other purposes are possible only upon agreement with the relevant structural unit head, under his/her responsibility.

4. Confidential, commercial, and official information

Information that contains commercial and official secrets is confidential.

The procedure for classifying information is described in ISMS.IT.PP.01 Information classification policy. The confidential information includes:

> 4.1. the order of access to computers, authentication data, business partners and customers of the Company data, program manuals, user manuals and other documentation, complete documentation on tasks, screens structure, files and databases description, flow charts of systems, other documentation, associated with the design, development and implementation of software;

4.2. information on the topology, network, and computing infrastructure of the Company, as well as technical means and systems for ensuring the security of information, are STRICTLY CONFIDENTIAL and not subject to disclosure;

4.3. lists of customers, names of representatives of business partners and customers of the Company, types of equipment and/or software that they acquire or use, as well as other related information;

4.4. ANY financial information, including financial terms of employees, partners or customers, information on the value of contracts, the financial and economic state of the Company, information on the cost of the equipment of the Company and its suppliers;

4.5. lists of potential customers, as well as information about contact persons of real or potential partners and customers;

4.6. lists of candidates, employees of the Company and information about them, including information on dismissed employees;

4.7. any information about research, developments, inventions, design, marketing activities, sales policy, and sales of the Company, which is considered as part of intellectual property.

The transfer of information of limited distribution containing confidential information to third parties without the written permission of the direct manager of the structural unit, or higher management is PROHIBITED. Required technical measures to ensure the confidentiality, integrity, and accessibility of confidential information are determined by the User.

Employees are obliged to prevent uncontrolled discovery of documents that contain confidential information, their printed form included. Employees are obliged to take all necessary measures to prevent their compromise by unauthorised users, copying, modification and loss, and are thus personally liable for these documents.

Transfer, processing, and storage of any information must not contradict the local legislation requirements.

5. Equipment maintenance terms

Employees are obliged to report anomalous behaviour of a computer, any identified changes in configuration, detected viruses, and other malfunctions (increased vibration, strange noises, smell, etc.) to the support service.

Employees are **prohibited** from:

5.1. Independently carrying out the modernisation and changing the configuration of equipment;

5.2. Uninstalling and stopping corporate firewall;

5.3. Uninstalling and stopping corporate anti-virus programs, installing alternative anti-virus software;

5.4. installing servers/services DHCP, DNS, WINS, and others, independently changing the computer network settings configuration (IP addresses, network name, protocols, and other parameters), including changing the settings of network adapters virtual environments by setting the Bridge mode (VMware, Virtual PC, etc.);

5.5. Using software designed to change the computer performance;

5.6. Installing and using other software included in the List of prohibited software;

5.7. Excluding a work computer from the corporate domain;

5.8. Deleting ITRANSITION\Service.WorkstationsOrganization, ITRANSITION\Domain Admins, ITRANSITION\SCCM.user from the local computer administrators group;

5.9. Allow unauthorised access to your PC data without the consent of your immediate supervisor;

5.10 Provide public network access to your PC data without authorisation to anyone. If necessary, public network access is provided only in the local network, only for defined persons and only for service purposes;

5.11. Carrying computers away (except for laptops, given to an employee in usage by the Company) from the office building of the Company without written permission of the administration;

5.12. Self-disconnecting/self-connecting any equipment to the uninterruptible power supply outlets in absence of a technical support engineer;

5.13. Disrupting seals (specially taped) of power sockets and plugs;

5.14. Leaving the workplace without taking measures to prevent information (by locking workstations) or hardware (mobile technology, laptops) theft.

In the event of a job-related necessity to deviate from one or more restrictions mentioned above (or of similar nature), it is necessary to consult the ServiceDesk service.

6. Corporate LAN, Internet and e-mail working terms

While working in the corporate network and the Internet, using corporate e-mail, it is **prohibit ed**:

6.1. To use traffic intercepting, hubs, and services scanning programs (sniffers, port scanners), as well as other software for unauthorised information access;

6.2. To deliberately install and use malicious software;

6.3. To deliberately attempt an unauthorised access to systems and subsystems of the Company, as well as to third-party information resources, including the use of software to launch attacks of any nature;

6.4. To use other Company's employees' accounts;

6.5. To independently connect any device to the corporate network (both wired and wireless), including personal equipment (with the exception of the "guest" net) without the consent of an authorised technical support engineer. Personal and non-standard devices may be allowed to be connected after prior approval from the structural unit head. Each device must be reconciled;

6.6. To independently organise remote access to the workplace and Company resources. In the event of the need to organise access to corporate resources from outside, a MDIS specialist installs special remote access software on an office PC or personal equipment, in accordance with the structural unit head;

6.7. To listen and to watch streaming media-content (TV, radio, movies), to transfer data by using Peer-to-Peer protocols for off-duty purposes;

6.8. To use e-mail as means of file transfer (message size more than 15 MB). For such purposes using specialised services (FTP) is recommended;

6.9. To use information systems, services, equipment, software, and hardware complexes of the group of Companies, including e-mail, for the development, testing, debugging, and support of software (including demonstration purposes), hardware, software, and hardware systems (except for systems specifically designed for such purposes);

6.10. To view the email of another person without his/her permission, without the appropriate authority, to allow another employee or an unauthorised person to use one's email address or system account, use the password of another employee or impersonate another person during messaging;

6.11. To send advertising and any other information of undesirable nature using the addresses and systems of the Company (spam);

6.12. Redirecting of corporate mail to external non-corporate systems and servers;

6.13. To independently, without MDIS coordination, connect third-party systems that interact with the information resources of the group of Companies, the corporate e-mail system and other published services and systems.

Note: *general security requirements are provided in ISMS.IT.PP.04 Network and Endpoints Protection.*

It is not recommended to turn on Wi-Fi standard radio transmitters (IEEE 802.11 protocols family), including the Access Point mode of personal mobile phones, tablets and the like, which are the source of the corporate Wi-Fi network jamming. Such actions cause the unstable functioning of corporate wireless equipment and make it difficult for users in the same frequency range.

7. The network print devices usage terms

When using network print devices it is **prohibited to**:

7.1. use damaged, perforated (including for binding), soiled, coated with correction fluid ("putty") and stapled paper;

7.2. place more than 250 sheets of paper in a printer;

7.3. disassemble or restart the printer without assistance, including extracting jammed /crumpled paper;

7.4. disconnect the printer from the local and electrical network;

7.5. open a paper tray of the printer during printing.

In case of a printer error, a repair request must be sent to the ServiceDesk service (ext. 911).

8. Company telephone network working terms

When using the telephone network of the Company it is **prohibited to**:

8.1. disclose or transfer a personal access code to anyone;

8.2. independently carry, disable, and connect telephones, modems, and any other equipment;

8.3. use the Company's telephone network for non-job-related purposes;

8.4. independently change telephone equipment settings;

8.5. carry phone equipment outside of the Company;

Notes:

- Rules and features of working with the telephone network of the Company are described in the "Company's telephone network working manual".
- The Company reserves the right to record any telephone calls in its telephone network at any time and to carry out other measures to control the targeted use of corporate services and equipment.