CETIN Hungary

COMPANY INTERNAL
Version No: 1.4
Valid from: 23.07.2021

Information Security Policy (Informatika Biztonsági Szabályzat)

		Job position/Name and Surname	Date (mm/yy)
Author(s)		KPMG / László Szűcs	07/2020
Process Owner		ISD / Levente Simon	07/2020
General Manager (CETIN Hungary)		CEO / Tamás Ötvös	
Supervision	Service Management		
	Compliance Management	Balázs Tóth Dr.	
	Security Management	Levente Simon	
Process		ISMS LEADERSHIP	

Revision history

Ver. No.	Revision category (draft, initial, update, main)	Author/Company	Main revisions	Revision Date
1.0	initial	László Szűcs	initial version	
1.2	update	László Szűcs	minor modifications / updates	12.07.2021
1.3	update	László Szűcs / Bálint Sándor Imre	corrections / updates	21.07.2021
1.4	update	SziT Ügyvédi iroda / dr. Spránitz Gergely	corrections / updates	22.07.2021

Approval history

Ver. No.	Approver name	Role	Date
1.4	Tamás Ötvös	CETIN Hungary / CEO	23.07.2021

Information classification

Ver. No.	Classification (Company Strictly confidential, Company Confidential, Company Internal, Open)	Classified by	Validity
1.4	Company Internal	László Szűcs	until next revision

Intellectual property rights

Contents

1. Abbreviations

1.1. Generic terms

Term	Description
CIS	Center for Internet Security
ISP	Information Security Policy
ISM	Information Security Management
T&C	Terms and Conditions
HLD	High Level Design
LLD	Low Level Design
BCP	Business Continuity Plan
DRP	Disaster Recovery Plan

1.2. Role related terms

For the sake of easier understanding of the policy the following table shows the CETIN Hungary naming convention as well.

Term	Description	CETIN Hungary Roles
ISO	Information Security Officer role	Security Director
IOL	IT Infrastructure Operation Leader role	Operations Director
SCOL	Server and Client Operation Leader role	Head of IT Infrastructure Services
NOL	Network Operation Leader role	Head of Transport Network Operations
SDL	Service Desk Leader role	Head of IT Infrastructure Services

2. Purpose and Scope

2.1. Purpose of the Information Security Policy

The purpose of the Information Security Policy (hereinafter: ISP) is to ensure during the operation and providing services of CETIN Hungary, the protection of the data managed, processed, forwarded and stored in the IT system in proportion to the risks (confidentiality, integrity and availability) from the potential sources of threats, in line with the requirements of the ISO/IEC 27001:2013 standards. The protection is independent of the place of origin, source, nature (personally received, original/copy, verbal/paper based/electronic, abridged/reworded/full) and form of these data.

2.2. Scope of the Information Security Policy

Information security policy has been built for determining high level concepts and directives of managing information security aspects of delivered services of CETIN Hungary.

2.2.1. Personal scope

The personnel scope of this policy covers:

- all employees of CETIN Hungary;
- all external organisations involved in service providing of CETIN Hungary in data processing;
- all legal entities and natural persons, including unincorporated entities participating in service providing of CETIN Hungary being in contractual relationship with CETIN Hungary;
- all communication with the organisations pursuing data exchange (sending and/or receiving, storing/forwarding) during service providing of CETIN Hungary in the framework of contractual relationship, independently of the role, place or location of the organisation, and its relation with CETIN Hungary.

2.2.2. Material scope

The material scope of this policy covers:

- all CETIN Hungary IT and telecommunication equipment and devices participating in its processes related to data management and processing, and the facilities accommodating those, irrespective of entitlement of use and their deployment method (physical or virtual, on-premise or cloud-based);
- all core and system software used for the operation of the IT and telecommunication equipment and devices dedicated for service providing of CETIN Hungary, as well as the application programmes and the documentation thereof (hereinafter: programme), irrespective of the ownership and deployment method (on-premise or cloud-based);
- all procurement, development, design and implementation works of the application systems and equipment used for service providing of CETIN Hungary;
- all contracts, registers, records and documents underlying the above;
- all data and storages being processed, stored, reached, transmitted, monitored or controlled thereon, or created as a result of the processing during service providing of CETIN Hungary, irrespective of their place of origin;

2.3. Issuing and structure of the Information Security Policy

The ISP document is approved and issued by the Security Director.

An Information Security User Manual shall be compiled for the employees, which contains regulations only applying directly to the employees.

The presentation of the regulations of ISMS to the external parties involved to providing CETIN Hungary is the responsibility of the contact person designated on behalf of CETIN Hungary.

2.4. Review of the Information Security Policy

Due to the continual changing of the statutory environment, the IT and information security standards and requirements, present Information Security Policy also must be periodically, *at*

least annually reviewed, or when any major change arises in the data processing system or in the laws.

In case of If any change initiated internally in the processes or systems regulated by the ISP, the Information Security Officer (hereafter ISO) must be notified in writing (which may be in the form of e-mail) for ensuring that ISO can review the change in terms of information security, and – when necessary – can initiate the change or review of the ISP.

ISO is in charge of the maintenance and review of the ISP.

2.5. Rules governing issuing, modification and management of Information Security Policy

The rules concerning the documents of CETIN Hungary, such as: issuing, format, structure, modification, version control, storage, retention and disposal are described in the Document Control Procedure of CETIN Hungary; accordingly this must be followed when preparing, modifying or managing the Information Security Policy or other documents dealing with information security.

2.6. Communication related to Information Security Policy

Referring to external and internal communication requirements and tasks related to information security, all parties involved must act in accordance with regulations of present policy.

3. Definitions

This document adheres to requirement definitions as described in RFC 2119 [1]:

Term	Synonym(s)	Meaning
MUST	REQUIRED, SHALL	The definition is an absolute requirement of the specification.
MUST NOT	SHALL NOT	The definition is an absolute prohibition of the specification.
SHOULD	RECOMMENDED	There may be valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood, documented and carefully weighed before choosing a different course.
SHOULD NOT	NOT RECOMMENDED	There may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood, documented and the case carefully weighed before implementing any behaviour described with this label.
MAY	OPTIONAL	An item is truly optional.

Further terms used in the document:

Term	Definition
Access	A procedure which makes the resources of an information system and the information stored on that system as data available to an information system user for a specific purpose (depending on the access rights of the user) and at a specific location and time.

Term	Definition
Access right	Providing possibility to perform activities in the information system.
Administrative protection	Protection implemented using organisational and regulatory means.
All-round protection	Information system protection is called all-round when it extends to all elements of the information system.
Antivirus system	Antivirus systems and related protection mechanisms are developed for finding viruses in information systems, preventing their operation and any active or passive damage they may cause, and - if possible - destroying them.
Asset	Anything which represents a value for the organisation. In this policy it means *data assets* (databases, data files, system documentation, procedures etc.), *software assets* (application and system software, development tools, etc.), *physical assets* (servers, switches, routers, central tools etc.) and any *services* supporting them (telecommunications services, public services etc.) and *human resources of CETIN Hungary*. In terms of ITIL asset is a configuration item (CI).
Authenticity	Information is authentic if its creator can be identified and the fact that it has not been changed since its creation can be proved without any doubt. Thus, authenticity is a data (and data storage medium) property, which can be used for verifying that the specific information provably derived from the expected source.
Availability	Information system state, which is true if system services can be accessed on a continuous basis or at a definite time or duration and the operability of the system is not hindered either temporarily or for longer periods.
Back-up media	A data storage medium (most often it is magnetic tape unit) which stores data content duplicated during back-up sessions.
Backup system	A system which is used to ensure data availability and to store program copies. The term is often used referring to an information system with minimum reserves.
Business secret	All information concerning to operation, business and business activities where the owner's legitimate interest to keep them secret, and where the owner has taken all necessary measures to keep them secret.
Business Continuity Planning	Keeping the availability of processes at a level where the organisation can tolerate the impairment, damages or loss caused by business disruption. (BCP – Business Continuity Planning).
Closed protection	The protection of an information system is closed if all relevant threats are taken into account.

Term	Definition
Confidentiality (state of the organization)	A state of the organization ensuring that data can only be accessed or disposed by those who are authorised for that. At a lower level confidentiality is a data property indicating that the protection measures prescripted by ISMS corresponding to the confidentiality category of the data are implemented.
Continuity	Uninterrupted availability of business activities.
Continuous protection	Protection kept uninterrupted despite of circumstances and relations changing over time.
Controls - precautions	Risk mitigating physical, administrative, technical and technological protection methods and procedures.
Cryptography	The theory and practice of hiding information from unauthorized access using mathematical algorithms, procedures and security rules.
Data	Data is the value of a specific property or attribute of an arbitrary object. E. g. if the chosen object is a person and the specified property is the colour of hair, the requested data may be e. g. "brown". Data per se has no meaning, only by operations being performed with it gains sense.
Data asset	Any entity comprising data
Data processing device	Any computing, telecommunication or other electronic device which can manipulate input data and generate output data as the result of the process and produce them in a form that can be interpreted by the person using it.
Data protection	The process of safeguarding data from corruption, compromise or loss.
Data security	A combined system of technical and organisation measures and procedures against the unauthorised access to, modification and destruction of data.
Data security breach	An act or negligence counteracting the security rules applicable to data protection and the consequences of which are a threat to the data.
Disaster	Interruption of the continuous and intended operation of the information system.
Disaster Recovery Planning	Planning how to recover the full operational capability after terminating or significant reducing of availability of the information system (DRP – Disaster Recovery Planning).
Electronic signature (digital signature)	A signal sequence generated by encoding and associated to data managed in the information system, which can be used to prove the authenticity and integrity of the data.
Encryption	Encoding a plain message using cryptographic procedure, device/tool or method.

Term	Definition
Hoax	A false alert sent by e-mail, which builds on the recipients' good faith and generates huge e-mail traffic, which in turn may slow down or disable complete mail systems. It does not contain any malicious codes. When it does, it is called a virus.
Homogeneity	Security covers all organization's activities, with same strength everywhere.
Illegal software	A software product which is protected by copyright but where there are one or more documents required to certify its legality (license, invoice, delivery note, donation contract etc.) are missing and the use of the software is not compliant with the requirements.
Information security	Maintaining data confidentiality, integrity and availability; other properties like authenticity, accountability, non-repudiation and reliability also belong here.
Documentation system	A multi-level overlapping system, which includes information security directives, todo's, participants, their tasks, rights, obligations and responsibilities; and also policies, processes, procedures, methodologies, technical work instructions, manuals and evidences of all activities.
Information system	A system of information, administration and business devices and procedures, and all electronic data processing devices and procedures supporting a process or the operation of a service, and all human resources and related processes servicing them. A combination of hardware, software and communication devices and organisations operating/servicing them and used by the financial institution to achieve its goals according to its business policy.
Incident	Any information-related event which is not part of normal operation. From information security point of view incident is a realized threat exploiting one or more system vulnerability.
Information Security Management System (ISMS)	Information Security Management System is intended to continuously develop the company's information protection system through regularly repeated planning, perforforming (doing), checking and acting processes (PDCA model).
Integrity	A data property indicating that the data is physically and logically complete, intact, accurate and have not been modified. Integrity also an information system property which is true if the information managed in the system and all other data processing system components can be modified only by authorised personnel.
Legal software	A software product which is protected by copyright and where all documents required to certify its legal use (license, invoice, delivery note, donation contract etc.) are available and the use of the software is compliant with the requirements described in the software licence agreement.

Term	Definition
Making a back-up	The process of making copies of data or data files to use in the event the original data or data files are lost or destroyed. For this process usually used a special tool, and special storage media.
Mobile device	Portable devices, such as: portable computers (laptops), PDAs, mobile phones, data storage media (USB pen drive etc.).
Mobile code	Also mentioned as RIA (Rich Internet Applications). Generally a software or code downloaded from a remote computer through the network and runs on the client computer without installation or launching the main program first. This category includes scripts (JavaScript, VBScript), flash animations, Java applets, MS Office document macros and ActiveX controls.
Network	A system of logical and physical devices accomplishing connections between computers (or, in more general terms: information systems) and data exchange between the various components of the connected systems.
Non-repudiation	Non-repudiation is a security requirement which refers to a situation where a statement's author cannot successfully dispute its authorship or the validity of an associated document. In other words it is a service that provides proof of integrity and origin of data.
Phishing	Illegal (online) data collection, data theft by deception of victims. It is expressly directed at acquiring personal data, e.g. login names and passwords, bank account numbers, credit card numbers, dates of birth. Its goal is to obtain data which can be used to obtain material benefits illegally. It often happens that potential victims are requested in an e-mail to resend their data or are called to send their password so that it could be verified. Data theft can occur through social engineering / deception, e.g. using a falsified web page (looking much like the original), by IP-address or link redirection, or by using technical methods, e.g. worms, Trojan codes or key-loggers.
Privileged access right	An extended user access right for special key persons necessary for performing special administering activities.
Protective measure	A measure taken using organisational or technical methods to mitigate impairment, damage or loss caused by a threat occurrence.
Protection system	A system of physical, logical and administrative protective measures used to guarantee the prescripted level of security of the information system.
Reliable operation	Reliable operation means that information systems (including the data managed by them) are available and their functionality are fully provided.

Term	Definition
Risk	Risk is a possibility to sustain impairment, damage or loss (in short: impact), can be caused by realization of a threat through a vulnerability of a system or a device. Accordingly the extent of a risk depends on impact and the probability of its occurrence.
Risk analysis	As risks consists of impacts and probabilities of their occurrence, and the probability of occurrence depends on threats and system vulnerabilities, risk analysis means assessment of impacts, vulnerabilities, threats and rates of their occurrence.
Risk management	Risk management means the following actions: Risk treatment: development, analysis and implementation of protection measures decreasing residual risks to an acceptable level. Risk avoidance: ceasing of the source of risk (e.g. service terminating, equipment disposal, etc.). Risk devolution: delivery of wearing risks to an external party (e.g. to an insurance company). Risk acceptance: issuing a management statement that the specified risk and its all consequences in case of realizing are perceived and being conscious of them the risk is accepted, no measure will be taken.
Risk-proportionate protection	Protection measure implemented on the basis of risk assessment and in accordance with risk level. This means that implemented measure suits the requirements of corresponding risk level, security level of measure is not unacceptable low, but not requires unnecessary resources. Risk-proportionate protection is always cost-effective.
Security	A state of the organisation in which owen to risk management procedures the risk level derived from the probability of occurring applicable threats and the possible impacts is acceptable. Security also a state of the information system, in which closed, complete, continuous and risk-proportionate protection measures are implemented. Security within information systems means that compliance with requirements and standards strengthening system operability, and the availability, integrity, confidentiality and authenticity of data.
Security requirements	Requirements of ISMS established in compliance with ISO/IEC 27001:2013 standard combined with requirements arised as result of risk assessment.

Term	Definition
Security event	Any event in the information system, service or network, which refers to possible violation of the information security policy, or the lack of security countermeasures, or any formerly unknown situation possibly related to security.
Security incident	Any realized threat exploiting one or more vulnerability of the information system. In ITIL terminology security incident is any information security-related event which is not part of normal operation.
Security classification	Security level assigned to a document, file, data or record based on the sensitivity or secrecy of the information. In CETIN Hungary four-degree classification is used: (1) Strictly confidential: needs highest degree of protection (2) Confidential: business secrets, unauthorized disclosure of which may undermine organization's business objectives (3) Internal: organization-specific informations, unauthorized disclosure of which may affect on market position of the organization (4) Open: for using with no restriction.
Security system	A means or method by which something is secured through a system of interworking components and devices.
Third person/party	Any person or organisation who or which has a contract with CETIN Hungary for participating in providing services and may access information system established for CETIN Hungary.
User	The person, organisation or group who (which) uses one or more information systems to carry out his tasks.
User authentication	Verifying the authenticity of a user (checking the identity of every user at login time) and using various authentication devices/tools (e.g. passwords, chipcards, biometric identification etc.).
Unauthorised person	A person who is not authorised to access the data.
Undesired mail (spam)	Irrelevant or unsolicited messages sent over the Internet, typically to a large number of users, for the purposes of advertising, phishing, spreading malware, etc. Such kind of messages often contain undesired intruders (viruses). The sender, the subject and the text of the messages change so often that it is not possible to filter these mails out based on a simple pattern.
Virus	Malicious program code which was written illegally as part of a user program. When its host program is executed the virus code can spread and 'infect' other system or user programs running on the information system, it can duplicate itself (which can produce mutant viruses) and by using the logic bomb effect it can also trigger a Trojan horse function based on some integrated condition (e.g. a special time, the number of free sectors on the hard drive etc.).

Term	Definition
VPN	A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. VPN technology was developed as a way to allow remote users and branch offices to securely access corporate applications and other resources. To ensure safety, data travels through secure tunnels, and VPN users must use authentication methods -- including passwords, tokens or other unique identification procedures -- to gain access to the VPN server.

Table 1 - Definitions

4. Responsibilities

The roles and responsibilities are declared in the ISM Strategy of CETIN Hungary.

5. Policy descriptions

5.1. Organization of information security

5.1.1. Segregation of duties

In order to reduce the possibility of the unauthorised or accidental modification or the misuse of the organisation's data assets the tasks and responsibilities must be segregated. It must be ensured that the same person cannot access, modify or use business critical data without proper approval and verification, or to complete the application and request approval process alone.

Incompatible jobs must be also segregated also in the information security organisation of CETIN Hungary:

- the verification of the compliance with the IT security rules shall be performed by the ISO, independently of IT operations;
- the internal auditor must be independent of the IT operation and of ISO;
- the system administering tasks of the internal system and the application servers, and the system administering tasks of the firewall and network segmentation shall be performed by different persons, who cannot substitute each other.

5.1.2. Contact with authorities

Proper relationship shall be developed and maintained with the external regulatory bodies and organisations responsible for information security. The purpose of keeping contact is to ensure fast and substantial cooperation in case of any critical information security event.

5.1.3. Contact with special interest groups

Participation in external professional information security groups, organizations is organized through cooperation agreements or through delegation of persons for cooperation events.

The purpose of the cooperation is to transfer knowledge, good practices, consultancy, process a specific topic, prepare suggestions, promote security awareness and event management.

5.1.4. Contact with other entities of PPF Group

CETIN Hungary service delivery shall be represented at a corporate level through established forums of the PPF Group.

5.1.5. Information security in project management

During conducting of each project, information security aspects should be enforced throughout the project life cycle. For this purpose Project Management should involve the ISO or Security Architects already in the planning phase and should keep informed about the information security aspects. IT security related costs must be also planned by the project.

The task of the ISO or Security Architects is to ensure that the electronic information system or system component of the project complies with the legal and information security regulations of CETIN Hungary.

5.2. Mobile devices and teleworking

5.2.1. Mobile device policy

Mobile information devices include e.g. notebooks, netbooks, smart phones, tablets and PDAs.

Both mobile information devices and the data stored on them must be protected against theft, unauthorised access and getting compromised.

5.2.1.1. Mobile device enrollment

Only company owned, company installed, enrolled and continuously managed mobile devices are allowed to connect to the network infrastructure of CETIN Hungary, whether on-premise or cloud-based.

Operating system of the device must not be modified in any way (e.g. "jailbroken") to give excessive access to the user.

Infrastructure Operation Leader (IOL) responsibility to ensure that "clean source principle" is applied, meaning that

- operating system of Mobile devices and the applications deployed to devices are obtained from trusted, approved sources and
- install media is verified via checksums after first retrival and before each usage to ensure installation media is not tampered with

5.2.1.2. Logical protection

Mobile devices are allowed to use exclusively by the user(s) assigned to it. Authorized users must not make the device available to use for other persons (e.g. friends, family) or anyone else without a written authorization from CETIN Hungary to use the device.

End-user computer devices (laptops, desktops) connecting to CETIN Hungary's network must meet the following security measures:

- Domain membership;
- Hardened and group policies applied;
- Up-to-date Antimalware System;
- Up-to-date operation system and used software patch state;
- Properly configured personal firewall;

- Software for full drive encryption of hard disks or built in memory cards of the devices and all other removable/portable media storage that may be connected;
- VPN software must be used for connection to CETIN Hungary's internal network that identifies both the connecting device and the connecting user by a certificate enrolled centrally.

Mobile device user's responsibility to report immediately to Service Desk if Mobile device is lost or stolen or if user suspects any unauthorised use of his/her assigned mobile device.

During remote working through public networks encrypted communication with strong authentication shall be provided.

All data classified as internal, confidential or strictly confidential (hereinafter: sensitive) must be encrypted when stored on portable computers / data storage media. The encryption software must be installed centrally on all notebooks. The encryption used must be configured to provide reasonable protection against unauthorized access to the data even for adversaries with physical access to the device.

Sensitive data must not be stored on portable devices which cannot be properly protected.

5.2.1.3. Physical protection

Employees using mobile devices must take all reasonable measures to keep the devices secure and maintain their integrity. This means the followings:

- Mobile devices carried out of office or home must not be left without control (even in closed car) while they are in public place. During travels mobile devices shall be carried in hand luggage, where possible hidden way;
- During storing mobile device at home it must not be left in visible from outside place;
- Outside of the secure zones mobile devices shall be used a way that performed activities could not be seen by third party;
- Manufacturer's directions concerning mobile devices always shall be adhered (e.g. mobile devices shall be protected against strong magnetic fields or using them near such fields shall be avoided);

Users are responsible for using portable devices handed over to them in accordance with the relevant requirements.

Only authorised persons are allowed to change the operating system and parameter settings of portable computers.

5.2.2. Teleworking

CETIN Hungary teleworking means granting remote access for operation purposes from networks which are not part of closed internal network of CETIN Hungary. Teleworking is available for all employees of CETIN Hungary.

For external users, remote access to information systems used for CETIN Hungary can only be granted in justified cases and based on the principles of need-to-know and least privilege. Limited remote access for external users can be granted proceeding an approval according to the Controlled Remote Access (CRA) procedure.

Remote access for support services provided by a third party, can be granted only to the supported systems and such access must be monitored. Not necessary connections must be disabled after finishing support activities.

5.3. Human resource security

5.3.1. Prior to employment

The security-related responsibilities must be described in the Job Descriptions which must be clearly communicated to the employees prior to employment.

5.3.1.1. Screening

It is the responsibility of HR and relevant area leaders that on their operation area applicants to be employed were

- screened in proportion with risks of role to be occupied;
- verified if applicant possesses skills, qualification and experience for job being performed;
- weighed from personality point of view (e.g. reliability, having responsibleness, commitment, being chargeable, ability to concentrate, ability to bear panic, etc.);

Screening of persons delegated by contractors or external parties for tasks related to CETIN Hungary in line with risks of work being performed is the responsibility of IT Infrastructure Operation Leader (IOL).

Screening must be performed in compliance with the laws, in an ethical way depending on the security level of the job, the sensitivity of the data to be accessed and the risk.

5.3.1.2. Terms and conditions of employment

As part of putting in force contracts (including employment contracts) employees of CETIN Hungary must sign their job descriptions and a statement about both the information security responsibilities of the employee and the organization.

Awareness of responsibility shall be a condition for working.

The declaration of the conditions and rules, as well as the contract must be in accordance with the organisation's information security regulations and should contain the following, as a minimum:

- all, contractual partners or external parties must sign a *confidentiality agreement* before starting the work and employees are required to accept an employment contract with non disclosure clauses;
- the *legal obligations* and rights of the employee, contractual partner or external party in respect of the *copyrights and data protection laws*;
- the responsibilities of the employee, contractual partner or external party concerning *classification of data* and *using of the organisation's assets*;
- the responsibilities of the employee, contractual partner or external party in respect of *handling of the information received* from other companies or external parties;
- the responsibilities of the organisation, as well as of the employee, contractual partner or external party concerning *handling of personal data*;
- the responsibilities applicable when performing work outside the organisation or outside the standard working hours, e.g. in the case of *teleworking*;
- the *measures* that can be enforced against the employee, contractual partner or external party upon *breaching the security requirements* of the organisation.

The obligations and responsibilities of the users are described in detail in the Information Security User Manual. The procedures which ensure that the employees, contractual partners and external parties understand their responsibilities and become capable of fulfilling the role for which they are employed must be elaborated mitigating the risk of thefts, frauds and malicious use.

The User IT Security Declaration must be prepared for employees, which shall contain:

- the user's declaration that he *learnt and accepted the IT security rules* relevant for him;
- that he *understands the expected and prohibited behaviour* during using IT systems, as well as the *sanctions* applicable to the breach of those.

The review of the User IT Security Declaration form wording shall be part of the review of present Information Security Policy.

5.3.2. During employment

5.3.2.1. Management responsibilities

The management must enforce compliance with the organisation's security regulations by all employees, contractual partners or external parties.

It is the responsibility of all area leaders on their operation areas, as a minimum:

- to provide proper information about employees' *information security responsibility* before granting access to sensitive data;
- to provide proper guidance concerning *security requirements* within the organisation employees need to comply with;
- to ensure that employees are adequately *motivated to adhere* the security regulations;
- to ensure that employees get the level of *security awareness* corresponding to their security role and responsibilities within the organisation;
- to ensure that employees' *behaviour corresponds to the declaration* signed in the employment conditions and rules;
- to ensure that employees continuously *enhance their skills* and obtain the qualifications necessary for the security and proper operation
- to ensure that any known or suspected security breaches or other security-related incidents that are brought to the attention of the manager are immediately reported to CETIN Hungary security.

Concerning contractual partners and external parties involved into providing CETIN Hungary services, the area leaders have the same minimum responsibilities as described above.

5.3.2.2. Information security awareness, education and training

For the purpose of supporting the organisation's security regulations and minimising the errors attributable to human mistakes it must be ensured during the work that the employees, the contractual partner or external party are fully aware of the security threats and issues, understand their responsibilities and obligations and all equipment necessary for the successful and secure performance of their work is available.

All employees, contractual partners or external parties must participate in security awareness training and they must be regularly informed of the changes of the security regulations and expectations, particularly of those that apply to their job.

The awareness training shall contain the following information about:

- information security rules and regulations (including detailed security requirements, legal responsibility, business controls, disciplinary process and training regarding the proper use of the data processing tools) and where these rules can be found;
- information security systems related to operation tasks and using of them (e.g. special applications registering operational activities);
- protection against malicious codes and activities (e.g. social engineering);
- actual threats and defence methods and techniques;
- perception, reporting and handling information security events;
- special knowledge referring to special working activities (e.g. assessment or other methodologies);

Information security training shall be delivered:

- for new employees of CETIN Hungary;
- for relevant users prior to implementing a new application or major modifications in an existing one;
- in case of significant changes of the regulations;
- in case of significant changes in IT environment;
- on such decision of Security Director;

Performing information security trainings and preparing training materials is the responsibility of the ISO.

Training records (e.g. participation lists, agenda, tests, etc.) shall be retained for audit purpose.

5.3.2.3. Disciplinary process

Proper disciplinary process must be established for security breaches. Establishing of the process and conducting inspections is the responsibility of the Security Director.

The following considerations should be kept in mind:

- disciplinary process may only be started when the fact of the breach has been confirmed;
- the employees suspected of the fraud must receive correct and fair treatment during the procedure;
- during the execution of procedure the nature and severity of the fraud, its impact on the business, whether it is a first time or recurring offence, whether the perpetrator received proper training, the relevant laws, business contracts and other factors shall be considered;
- evidence must be preserved and it must be ensured that if necessary, such evidence is handled in a manner so as to keep it court admissible;
- in severe cases all access rights of the perpetrator must be immediately revoked, all company-owned assets recovered and the Security Director together with HR

Director decides whether the perpetrator must immediately be escorted out of the building.

5.3.3. Termination and change of employment

Upon termination of employment or changing of it impacting employee's duties, it is the responsibility of HR:

- to clear the remaining responsibilities;
- course of returning assets;
- way of revoking access privileges
- secure removal of all corporate data and settings from any device that the employee may decide to keep, either locally or remotely using the appropriate tool for this purpose (e.g. by issuing a retire command in the mobile device management tool)

The responsibility of the Infrastructure Operation Leader (IOL) to ensure that the employee's access rights are revoked or modified.

The Server & Client Operation Leader (SCOL) must perform the following tasks in this regard:

- He must backup and archive the electronically stored data, e-mails and other data created by the user (in connection with his work) from the IT device, server location or other storage used by the employee.
- The archived data must be stored in accordance with the statutory provisions and, if necessary, deleted from the system after the expiry of the specified period.

It is the responsibility of the departing employee's direct supervisor to ensure business continuity, including retaining access to critical business information that may have only existed in document stores under the control of the employee, and also notifying all affected partners about the personnel change, clearly communicating the departing colleague's substitute who should be contacted in the future.

The employee must be made aware of the responsibilities and tasks related to the resignation, which should cover the security requirements and the legal responsibility.

The modification of the employment conditions must be treated as if the employee's previous responsibilities ceased and the activities related to the new position must be performed in accordance with the "Prior to employment" chapter.

5.4. Asset management

5.4.1. Responsibility for assets

5.4.1.1. Inventory of assets

The asset inventory must cover the following areas, as a minimum:

- Primary assets:
  - Business processes;
  - Information;
- Supporting assets:
  - Hardware;
  - Software;

- Personnel;
- Site;
- Organization.

The asset inventory shall contain the following data regarding to each asset:

- Asset: name and description of the asset;
- Owner: The person responsible for the management of the asset (the ownership defined herein is not identical to the ownership in a legal scence);
- User (applicable only for hardware and software assets): name of the user assigned to the hardware and the software asset;
- Note (not mandatory): other relevant information.

The proper design and continuous maintenance of the asset inventory are the responsibility of the IOL.

5.4.1.2. Ownership of assets

Each information system (and related assets) used in CETIN Hungary must have a designated Owner.

5.4.1.3. Acceptable use of assets

Assets used for providing CETIN Hungary services are dedicated for service delivery with the following limitations:

- it is only available for use by approved users;
- the level of use must be reasonable and not detrimental to the mission of the CETIN Hungary;
- priority must be given to use of resources for the main purpose for which they are provided;
- personal use must not be for a commercial purpose or for personal gain;
- personal use must not be of a nature that competes with CETIN Hungary's business;
- personal use must not be connected to any use or application that conflicts with an employee's obligations to CETIN Hungary as its employer;
- personal use must not be connected to any use or application that conflicts with CETIN Hungary's rules, regulations, policies or procedures, including this policy;
- it is a privilege that may be withdrawn at any point.

Additionally:

- CETIN Hungary does not accept any liability for damage or loss of whatever nature caused by the use of the email service for personal purposes. This exclusion does not apply where personal injury or death is caused by CETIN Hungary's negligence.
- Users of assets dedicated for providing CETIN Hungary services must not do anything to jeopardise the integrity of the Information Systems by, as follows:
  - Damaging, reconfiguring (e.g. disabling the anti-virus) or moving equipment (desktop PCs, printer s, scanners and monitors);
  - Loading software on the equipments other than in approved circumstances;

- Reconfiguring or connecting equipment to the network other than by approved methods;
- Setting up servers or services on the network, or installing software on workstations without approval;
- Deliberately or recklessly introducing malware;
- Attempting to disrupt or circumvent any Information Security controls;

Additionally, all persons in the personal scope of this policy must not:

- infringe copyright, or break the terms of licences for software or other material;
- attempt to access, delete, modify or disclose Information Assets belonging to other people without their permission, unless it is obvious that they intend others to do this;
- access, create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist. CETIN Hungary reserves the right to block or monitor access to such material. If such material is accessed accidentally, advice and guidance should be sought from their service operation leaders. There is an exemption covering authorised Information Security and IT Operation staff involved in the preservation of evidence for the purposes of investigating breaches of the regulations or the law.
- use information assets in a manner that unnecessarily takes up capacity, wastes staff effort or other IT resources, weakens the performance of the information system or poses a security threat;
- send unsolicited bulk or 'marketing' emails (junk) or chain emails;
- use provided by CETIN Hungary email address to register on websites that are not connected with providing CETIN Hungary services (e.g. online auction, gambling or similar websites);
- disrupt the work of other users, deny them access to services, or corrupt or destroy their data.

The owner of the asset is responsible for:

- Registering the asset in CMDB (Asset Inventory);
- Allocating the data related to the data processing device to the appropriate classification category;
- Ensuring the asset is kept secure throughout its life cycle, including the timely installation of all necessary security updates;
- performing the tasks related to access protection and categorisation activities:
  - assessment of access rights;
  - review of access rights;
  - regular or ad hoc review of data classifications;

The user of the asset components is responsible for:

- adhereing rules for mobile devices and teleworking;
- adhereing rules in course of handling internal, restricted or confidential information;
- reporting the malfunction of the asset immediately via the Service Desk
- seeing to the protection of the asset's condition and its proper use

- in the case of mobile devices seeing to the continuous supervision thereof
- in the case of mobile devices, keeping the device secure at all times by a timely installation of all security updates.

Data assets of CETIN Hungary may only be accessed from, managed or stored using devices that have been authorized (in writing) for this purpose by the ISO and the IOL. Access, transmission or storage of such data assets using unauthorized devices and/or devices without appropriate security controls is prohibited.

5.4.1.4. Return of assets

In case of termination agreement with CETIN Hungary all assets used for providing CETIN Hungary services must be returned in their possession to CETIN Hungary.

The process of terminating must ensure that all software, documentations, mobile devices, bankcards, security passes, manuals, electronically stored data or tools used for providing CETIN Hungary services are returned to CETIN Hungary. The process must be established by the Human Resources.

When returning a device or equipment, it must be checked whether the user returns the asset with the hardware and software specification he received and registered, in good working order.

5.4.2. Information classification

In order to ensure proper (risk-proportionate and cost-effective) protection, information managed in the IT systems of CETIN Hungary must be classified in a way that reflects the value and importance of the information, and extent of the required protection.

5.4.2.1. Classification of information

Information shall be stored using information security homogeneity principle.

Information security measures applied to an information set must be matched to the most sensitive data.

The size of the potential damage arising from the loss of the confidentiality and integrity, or the availability of the data must be also taken into consideration for the purpose of the classification.

At the initiative and under the coordination of the ISO the IOL reviews the classification at least once a year and either changes or approves the classification, when:

- a new IT application or system is being implemented;
- an IT system is being modified, if the modification impacts the range of the managed information;
- any change occurs in a business process which also impacts the range of the information managed by the respective business process;
- a new data group appears as a result of the statutory, legislative changes;
- when a new module is integrated into an existing system.

CETIN Hungary differentiates four classification categories:

Information protection class	Typical data or information types

Strictly confidential	Highly sensitive information, available only for narrow circle of responsibles concerning IT infrastructure and environment of CETIN Hungary (e.g. results of vulnerability scans or penetration tests, configurations of active network devices, fallback passwords for IT systems, etc.)
Confidential information	Sensitive information, available for extended circle of responsibles concerning IT infrastructure and environment of CETIN Hungary (e.g. network segregations, ip addresses, HLD and LLD documentations, etc.)
For internal use only	Information available for all employee of CETIN Hungary (e.g. regulatory documents, policies, procedures, etc.)
Public information	Information accessible for anyone (e.g. information can be forwarded for external parties)

Table 2 - Information classification categories

Information classification is the responsiblity of ISO.

5.4.2.2. Labelling of information

Code	Information protection class	Label in CETIN Hungary
DS1	Strictly confidential	Company Strictly Confidential
DS2	Confidential information	Company Confidential
DS3	For internal use only	Company Internal
DS4	Public information	Open or no label

Table 3 - Information classification labelling

The classification must be indicated on the documents prepared by computer; in the case of documents – also including the electronic documents – in the header or footer of each page (sheet).

The classification of a data asset is always determined based on its content. The lack of labeling of a data asset does not necessarily mean that the particular data has been classified as "open", and therefore the fact that a document is not labelled does not automatically grant the right for anyone accessing such data to publish it, or to make it otherwise known to the public.

5.4.2.3. Handling of assets

Asset handling must be performed in accordance with principles described in attached excel document in Appendix 7.1.

5.4.3. Storage Media Handling

5.4.3.1. Management of removable media

The protection of the replaceable computer storages (such as tapes, disks, cartridges and data storage CDs/DVDs, external hard drives and pen drives) takes place as follows:

- the data content of the recyclable, but not necessary for CETIN Hungary any longer, storages must be erased in a non-recoverable manner;
- the storages must be stored in a safe environment that also satisfies the manufacturer's environmental specifications;

- unless a security exception is granted in writing by the ISO (after a risk analysis), all data that is stored on removable media or portable data storage devices must be protected against unauthorized access using strong encryption;
- a copy must be taken of the data to be stored longer than the lifetime of the storage specified by the manufacturer and it must be delivered to another site in order to prevent data losses attributable to the aging of the storage;
- the storages storing the duplicate of the archives and backups must be kept in a strongbox accessible by authorized persons;
- a register must be kept on the storages to prevent data losses from accidental deletion/destruction;
- the use of mobile storages may only be authorised subject to proper business justification.

Ensuring that the above rules are followed is the responsibility of the IOL.

5.4.3.2. Disposal of storage media

Sensitive data (i.e. not data explicitly classified as Open) stored on storage devices no longer in use must not be obtained by unauthorised persons. Therefore, the storage devices that are to be decommissioned must be withdrawn from use in a safe manner. Documented procedures must be developed for the safe removal of the storages.

During the procedure the following aspects should be considered:

- paper-based documents (including the system documentations) must be shredded (by a cross-cut document shredder satisfying DIN 66399 P-3);
- single-user printer tapes must be physically destroyed (by burning);
- magnetic tapes must be erased by a demagnetising equipment or destroyed physically;
- the electronic storages containing data of DS1 and DS2 class may be used for other purposes only after deletion and overwriting them several times with randomly generated data using the total storage capacity of the storage. If this is not feasible, then the device must be scrapped and destroyed;
- faulty mass storage units (hard disk) must not be replaced even in the framework of repair under warranty or released in any form, if it contains interpretable data or data that can be restored from the unit;
- if the destruction is performed by subcontractors, the service may only be used subject to written contract with a service provider that has appropriate security certifications, and such contract must always contain the confidentiality agreements and the right to audit, as well;
- the destruction of electronic storages or of registered paper-based documents must be documented in minutes.

Process of physical destruction of storages:

- A summary list of the storages to be destroyed (magnetic tape and cartridge, CD, DVD, HDD, SSD, etc.) must be prepared, which contains the following information:
  - exact type of the storage;
  - serial number or unique identifier (if any) of the storage;

- type and purpose of the data stored thereon (e.g. in case of software the name of the software, in case of database the function of the data, etc.);
- the IOL's approval.

- The ISO will supervise the proper stow and destruction of the storages.

5.4.3.3. Physical media transfer

During transportation, storage devices must be protected from unauthorised access and harmful physical impacts.

When transporting data storage media (CD/DVD, tape drives, external drives) between sites, the following must be borne in mind:

- Devices can only be transported using a reliable forwarding agent or courier;
- the management must approve the list of authorised couriers;
- a procedure must be elaborated for the identification of the couriers;
- appropriate packaging must be used that protects the content of the storage device from harmful impacts arising during the transport (e.g. overheating, vapour condensation) and tampering; the applied packaging must satisfy the manufacturer's recommendations;

The transport of storage devices outside the building is subject to the ISO's approval, who must see to the proper transport conditions.

5.5. Access control

5.5.1. Business requirements of access control

5.5.1.1. Access control policy

The objective of access control is to ensure that every user can access only those computer data, programs and services available in the information systems used by CETIN Hungary which are absolutely necessary for them to do their job. Access control shall cover all phases of the user life cycle (starting with registering new users in the systems until their final deletion from the registry), and to define the general requirements for controlling data access in information systems used by CETIN Hungary.

All systems and devices storing CETIN Hungary data must be subject of centrally managed access control – whether on-premise or cloud, physical or virtual, company-owned or owned by another entity, and whether the users are employees of CETIN Hungary or external parties.

To ensure the confidentiality and integrity of the data stored in data processing systems, user access groups/roles must be set up and managed taking into account all business and security requirements, following a RBAC (role-based access control) method.

To complement the access controls, an identity authentication mechanism must be in place for each information system used by CETIN Hungary that can ensure that all access to such systems are data can be unambiguously traced back to the individual who accessed it.

Permissions / rules applicable to each user group must be clearly defined.

The following must be taken into account when setting up user access groups:

- security requirements of specific business applications;
- confidentiality of data stored by business applications and the related risks;

- they should be in line with the security classification rules applicable to the data;
- legal regulations in force;
- separation of access control roles;
- requirement for the formal approval of user access;
- regular review of access rights;
- removal of unnecessary access rights;

Physical and logical access needs to be managed in an integrated manner, taking their interrelations into account.

Access to applications must be limited in line with the principle of necessary and sufficient access (also known as "need to know, need to do" and "least privilege") and the conflict of interests regulations (segregation of duties, or SoD).

5.5.1.2. Access to networks and network services

Users may be granted access only to those services that they have explicit access rights to. These access rights are approved by the resource owner and set by the relevant IT Operation Team members under the leadership of the IOL.

5.5.2. User access management

5.5.2.1. User registration and de-registration

Procedures must be developed to manage user access rights. These procedures must include user registration as well as the application for, modification and revocation of user rights. These processes must be extended to cover the management of user access rights associated with applications, database management solutions, operating systems and remote access. Special attention needs to be paid to revoking the user rights of those leaving the company within as short a time as possible.

Basic level user access (login name, password) and user access to applications and systems can be applied for through a formal process.

5.5.2.2. User access provisioning

Unauthorised access to information systems must be prevented. Granting access rights to information systems and services must be controlled through a regulated process.

The procedure covers each stage of the user access life cycle starting from the initial registration of new users till the access right is finally revoked. Granting privileged user access rights must be closely controlled.

Logged processes must be developed to store and use passwords not used for daily work, and by nature granting full access to system operation (e.g. system administrator fallback passwords, active directory restore passwords). Such emergency access methods must not be used for daily operation and all such use must be closely monitored.

5.5.2.3. Management of privileged access rights

Granting privileged access rights must be preceded by a more stringent authorisation process than that required for standard user access rights. The procedure implemented must fulfil the following criteria as a minimum:

- the system elements (e.g. operating systems, database management system and applications) and the employee categories that the administrator access rights are to be associated with must be defined in detail;
- administrator access rights must be granted based on the principles of "absolutely necessary" and "event-based" use;
- all user right requests must be documented;
- user identifiers used for administration must be distinguished from those used in daily work;
- system operation procedures must be implemented in a way which minimises the use of privileged user access;
- services and programs must be developed to run without requiring any privileged user access;
- any activities performed with privileged user access must be always logged;
- system administrators must not abuse their access rights to invade on other's privacy, view users' personal details, nor are allowed to send letters in the name of other users or in any other way impersonate other users.

5.5.2.4. Management of authentication secrets of "standard" users

Authentication of standard users is primarily based on username/passwords. However whenever it is possible authentication must be supplemented by certificate based or other multi-factor authentication technology (MFA).

Only MFA technology that is explicitly authorized by the ISO shall be used.

Certificates must be created:

- upon provisioning all computers into Active Directory a computer certificate must be assigned identifying the computer
- upon creating a "standard" user account in Active Directory a user certificate is created identifying the user.

The following must be observed in the course of user password management:

- Users must change their initial password after logging into their user account for the first time, and every time they receive an initial password that someone else sets for them, to ensure their password is only known to them and no one else.
- Passwords must be kept secret, therefore, to this end:
  - It is forbidden to tell others the password, or to speak about the password in the presence of others;
  - The password must not be revealed even to superiors, system administrators or administrators, not even when the user is expressly requested to do so;
  - It is forbidden to use common passwords (not even if it is shared with a family member or a friend);
  - Passwords must not be written down and kept in an easily accessible place (in the office, in a briefcase or bag etc.);
  - Do not refer to the content of the password (e.g. 'it is my favourite band');
  - Do not use the 'Remember my password' function offered by various software;

- It is forbidden to use technologies that weaken password protection, including password reminder hints and "security questions" functionalities.
- If the login name and the password must be sent, the elements of the user name / password combination are to be sent in separate channels (e-mail, postal mail, text message). The message including the password must not contain any information as to the user name and the system it can be used with.

- Passwords must be difficult to guess but easy to remember, must not be based on personal data (e.g. they should not contain telephone numbers, the child's name, date of birth, the name of a favourite pet, a company name, a licence plate number etc.) and must not be a word that one could find in a dictionary. Users shall be instructed to use longer, easy to remember passphrases instead of hard to remember and less secure passwords.
- Users are obliged to change their password in the shortest possible time if there is any suspicion that others might have gained knowledge of their password. If this is even suspected, it must be reported by the user immediately and investigated as a security incident.
- Users must not ask other users about their passwords or use another user's ID after that other user logged in. Similarly, a user must not allow other users to use his ID or let others use his account after logging in.
- Passwords used to access CETIN Hungary's systems must not be used also to access third-party systems (e.g. Gmail).
- Forgotten password replacement procedures must be documented and all password replacement events must be logged.
- If a user forgets the initial or his current password, he must be clearly identified before a temporary password can be issued to him.
- All initial and temporary passwords must be forwarded to users via a secure channel.
- Initial and temporary passwords must be unique.
- It is forbidden for users to run any application capable of hacking passwords. If this is necessary, for example, to check password quality, the ISO's consent needs to be obtained prior to that.

Protecting the user's account and in particular, keeping their authentication data (such as passwords or PIN codes) confidential and their authentication devices (if used) protected from unauthorized use are the responsibilities of every user. All users are accountable for actions performed using their identifier, regardless of who actually used the account, unless the given user can prove that they have done everything in their power to protect the account and an abuse of their account was through no fault of their own.

5.5.2.5. Management of authentication secrets of privileged users

Privileged users must always authenticate themselves when accessing systems with strong multifactor authentication if the system supports strong multifactor authentication,

- the 1st factor of authentication can be username/password
- the 2nd factor must be a true physically disconnectable device (e.g security token storing private key of privileged account, one-time password generator, etc.)

Security tokens must not be shared among administrators, nor with anyone else. Such authenticators must only be used by their registered, authorized user.

5.5.2.6. Review of user access rights

User access rights must be regularly reviewed to terminate unjustified or unnecessary user access.

Every user access right granted for business applications must be reviewed annually.

Concerning reviews, it must be documented who initiated them and who undertook them, as well as a clear indication of the explicit confirmation or cancellation of access rights and the confirmation of any cancellation.

Access right reviews are managed by the ISO.

5.5.2.7. Removal or adjustment of access rights

The access right of the employees or external parties must be suspended, revoked or modified upon resignation or position change, respectively.

The execution of the prescribed tasks is the responsibility of the IOL.

5.5.3. User responsibilities

In order to prevent unauthorised user access, users must be made aware through regular courses of their responsibility for maintaining efficient security controls, with special attention paid to password use and user equipment security.

To maintain the hardware and software integrity of all data processing equipment owned by CETIN Hungary, users are forbidden:

- to install any software components on the computers unless explicitly authorized;
- to physically open the computer cases: to replace, install or remove computer parts.

Users with login access rights MUST NOT log into CETIN Hungary systems or network using another user's card, security token or identifier.

Workstation use must not be transferred to anybody when the unauthorised use of the workstation functions may compromise information security.

When naming files (i.e. when saving them), they must be given unique names not containing accented characters and preferably referring to the content of the respective file. In the case of materials prepared in more than one step, each version must be assigned a separate version number.

5.5.4. System and application access control

5.5.4.1. Information access restriction

See chapter Access control policy.

5.5.4.2. Secure log-on procedures

Login details must be protected while information services are used. Protective measures must extend to the following:

- the system or application identifier should not be displayed until the login process is successfully completed;

- a warning should be displayed for users trying to log in without proper authorisation;
- login data should be validated only when all data have been input;
- when incorrect data are input, the system should not identify correct and incorrect data;
- it should limit the number of unsuccessful login attempts; the identifier should be locked for at least 30 minutes after 5 consecutive unsuccessful login attempts, except when there is a special permission ruling otherwise;
- login password management should comply with the content of the Password Management system chapter
- unsuccessful attempts should be logged.

Compliance with the above criteria must be achieved through system parameter settings. It is the IOL's duty and responsibility to ensure that all settings are appropriate.

5.5.4.3. Password management system

The use of passwords is a fundamental access control tool, one of the cornerstones of information security.

A password quality control solution needs to be introduced for every information system. This is the responsibility of the IOL.

Minimum password requirements for user accounts:

- The password cannot be the same as the name of the user account;
- Passwords must be at least 8 characters long and contain 3 of the following character types as a minimum: upper case letters, lower case letters, numbers and special characters;
- Passwords can remain valid for no longer than 180 days after they are changed;
- When changing passwords, users cannot select any of their 10 most recently used passwords.
- New passwords can only be changed after one days have passed;

Minimum password requirements for system administrator accounts:

- The password cannot be the same as the name of the user account;
- Passwords must be at least 12 characters long and contain 3 of the following character types as a minimum: upper case letters, lower case letters, numbers and special characters;
- Passwords can remain valid for no longer than 180 days after they are changed;
- When changing passwords, system administrators cannot select any of their 10 most recently used passwords;
- In the case of information systems which do not provide means to technically enforce compliance with the above requirements, it is the system administrators' responsibility to use passwords meeting the expectations, and they are also responsible for any damage caused.

Minimum password requirements for system accounts (OS, DB, interface):

- They are the same as the requirements applicable to system administrator passwords, except that it must be at least 16 characters long, it is sufficient to change these passwords annually and password expiration does not need to be automated;
- the process (steps) of changing the passwords must be documented;

Persons with access to more than one system or having multiple user IDs must use different passwords for the different systems and identifiers.

The ISO must review or have someone review the information systems not meeting the above criteria.

Passwords must not be displayed during input.

Users must be provided the possibility to change their passwords whenever others have learnt or are suspected to have learnt their passwords.

Passwords must not be recorded/stored in audit log files, system log files or error log files.

Information systems must store passwords in a form that prevents their decryption and protects them from unauthorised access, e.g. passwords must not be stored in plain text format in data processing systems.

Initial passwords (e.g. the ones set when creating a new user account or when resetting a password) can only remain valid until the first successful login, when in turn the system must enforce changing such passwords; if the system is not capable of that, it is the system administrators' responsibility to enforce a password change. Initial passwords must be unique and difficult to guess.

Default passwords must be changed when the equipment is installed.

It is not allowed to code passwords into scripts, batch files or configuration files, except when a more secure method is technically not feasible and even then, only if access to such files is limited to the necessary minimum.

If the system supports forwarding passwords in an encrypted form, this service must be used to prevent intercepting passwords while they are being transmitted through networks.

5.5.4.4. Use of credential manager applications

Users and administrators are only permitted to use password/credential manager applications (either locally installed ones or centralized) that have been reviewed and explicitly approved for this purpose by the ISO.

It is explicitly forbidden to store passwords in documents, text files or other formats that are not explicitly designed for secure password storage. The browsers' built-in password storage functionalities must not be used.

Passwords and account information granting access to corporate systems and data must not be mixed with account information for private (non-organizational) systems or data.

Corporate account information and passwords must not be synchronized to cloud services which are used for private purposes (e.g. the iCloud keychain of the employee's private Apple ID).

5.5.4.5. Use of privileged utility programs

The system must prevent privileged users from running programs which are not part of the operating system and can render the authentication procedures or the protective functions used on the computer or by the various software ineffective. If the applied technology allows it, the use of such programs must be limited or made impossible.

Running and all activities of privileged utility programs shall be logged and parsed and event notification shall be sent to Information Security responsibles.

Any deviation shall be reported to ISO who is responsible to decide what action needs to be taken.

5.5.4.6. Access control to program source code

The source program package must be stored separately from the development or the live system, with live and earlier versions clearly separated from each other. Only SCOL or his/her delegates may have access to the directories storing live source program files.

5.6. Cryptography

During providing CETIN Hungary services it might be required to use encryption and message validation applications for communication within its internal systems and with its customers and contracted partners.

5.6.1. Policy on the use of cryptographic controls

With regard to the cryptographic tools used in CETIN Hungary service delivery, a regulation must be drawn up to guarantee their secure use:

- the requirements ensuring their protection;
- the requirements related to their use;
- the rules for generating, distributing, storing and destroying the keys;
- the rules and procedures for the recovery of encrypted data in cases where the key has been damaged or lost.

Only such cryptographic solutions are allowed to be used to protect category DS1 and DS2 data in information systems:

- which are compliant with applicable standards of actual version of *FIPS 140-2 Annex A* or
- which is used based on the ISO's approval.

5.6.2. Key Management

The method of protecting cryptographic keys must by developed in the regulations providing for the secure use of cryptographic devices and/or tools, before the live operation of the specific system begins.

In line with the applicable standards or requirements accepted as standards, appropriate (e.g. PKCS, FIPS 800-57 compliant) key management systems can be used. Internal requirements must be specified in the cryptographic instructions or in the descriptions of the relevant application.

Since the loss of a decryption key can render all data encrypted using the corresponding key permanently irrecoverable, it is strictly forbidden to use any data encryption without sufficiently secure and documented key management processes which ensure that the encrypted information can be successfully decrypted by those (and only those) persons that are authorized to access it.

5.7. Physical and environmental security

5.7.1. Secure areas

5.7.1.1. Physical security perimeter

The premises of different security classification must be separated by security lines.

All physical security perimeter protection must be designed following a thorough assessment of all relevant threats, either natural or man-made.

When designing the security lines the following principles must be observed:

- the designation of the security line must be clear;
- the security line of the site or building on its own must provide a homogeneous level of protection, i.e. there should be no gap or any part where it is easy to get through;
- the protective walls must be solidly built;
- the premises must be equipped with security doors that prevent unauthorised access, e.g. mechanism, bars, alarms, bolts;
- the physical access to the site or the building must be controlled by manned access gates;
- the physical obstacles – where the security requirements justify it – must be extended from the floor to the ceiling to prevent unauthorised access or other environmental damages, e.g. fire or flood;
- the fire doors must be swing-doors equipped with alarm.

5.7.1.2. Physical entry control

The security of the business sites must be protected by such access control which ensures that only the authorised personnel can enter.

When implementing the access control solutions and procedures the following security measures must be enforced:

- The visitors of the business sites must be continuously supervised and escorted; the date and time of their arrival and departure must be recorded. Visitors must be provided with access that is valid only for the preliminarily agreed time and location. The visitors must be familiarised with the rules applicable to the security requirements of the business site and the procedures to be followed in case of emergency.
- Access to sensitive data and data processing tools must be controlled and restricted to the authorised personnel. The authorisation and validation of access must be subjected to authentication security measures (such as security card supplemented with a PIN). The access control routes must be managed securely.
- The security guards must be informed of unescorted outsiders or visitors, wandering around. Such persons must be escorted out of the building.
- The access rights valid for the business site must be kept up-to-date by regular review.
- Access logs must be regularly reviewed.

5.7.1.3. Securing offices, rooms and facilities

In order to protect sensitive data and systems from unauthorized physical access, modification or loss, the ISO designates secure areas.

The secure area means the office part or group of premises within a single security line, which can be either locked or which contain lockable cabinets and strong boxes. When selecting and designing the secure area all potential damages that may arise from fire, flood, explosion, civil riot or any other form of natural or human inflicted disasters must be taken into account; at the same time the effective health and safety regulations and standards must be also borne in mind. When designing the protective measures the broader environment of the secure area must be also considered – e.g. the characteristics of the neighbouring buildings or premises – in order to eliminate the environmental effects, such as water pipe bursts or leakages, arising elsewhere.

Secure areas must be clearly identified and visibly marked as such.

The following security measures must be implemented as a minimum:

- observing the health and safety requirements
- the unused data processing device must be placed in a lockable cabinet
- catalogues and internal directories that may contain information on sensitive data processing tools must be protected from public access
- the auxiliary equipment and tools, such as copiers and faxes, must be suitably placed within the secure areas
- the windows and doors must be closed if no supervising personnel is nearby; the external physical protection of the windows must be also ensured, especially on the ground floor
- an appropriate intrusion detection system must be established in accordance with the relevant industry standards, the operation of which must be regularly reviewed to ensure that it covers all external doors and accessible windows the uncontrolled secure areas – e.g. computer room or telecommunication devices – must be equipped with permanent alarm
- a fire extinguishing system or tools suitable for firefighting must be provided for the devices, in addition to the fire alarm, which cause no harm in the electronic devices
- the persons in the premises must not take any photo, video or voice recording in the premises, unless the ISO authorises this in writing
- the work premises must be protected by card-controlled access system
- no external parties are allowed entry to the secure areas without escorting, unless explicitly authorized in writing by the ISO.

5.7.1.4. Protecting against external and environmental threats

CETIN Hungary must take precautions against losses arising from fire, flood, storm, earthquake, explosion or civil riot, and against the direct or indirect effects of other natural or human inflicted disasters.

The precautionary measures must take account of the following:

- hazardous or inflammable materials must be stored securely in safe distance from the secure areas;
- goods delivered in bulk – e.g. office stationery – must not be stored in the secure area

- the backup equipment and reserve storages must be placed in a secure distance that precludes their damage in the event when the central site is hit by a disaster
- fire extinguishing equipment that satisfies the security protection requirement of the given premises must be installed

When designing environmental protections, in addition to preventing the physical loss of assets, ensuring the continuous, uninterrupted operation of business and mission critical services must also be considered.

5.7.1.5. Working in secure areas

In order to enhance the safety of the secure areas additional precautionary measures and guidelines may be necessary. As a minimum compliance with the following requirements must be ensured:

- the personnel should have access only to the areas necessary for them for the performance of their work and they should be able to perform only those activities there that are necessary for their work ("need to know principle");
- unsupervised work in the secure area must be avoided for the sake of security and for the purpose of precluding the possibility of malicious activity;
- if there is nobody in the highly secure area the area must be safely locked and it must be regularly checked that indeed there is nobody inside,
- photo, video and audio recording must not be permitted, or it should be subject to special authorisation,
- upon entering the secure area it must be checked that only those electric devices are with the person performing the work that are necessary for the work.

5.7.1.6. Delivery and loading areas

The delivery and loading zones must be controlled and, if possible, they must be isolated from the data processing equipment to prevent unauthorised access. The security requirements of these areas must be determined based on a formal assessment of risk.

The following precautionary measures should be taken into consideration, as a minimum:

- restricting the access to the storage area outside the building to the identified and authorised personnel;
- the storage area must be designed in a way that permits the loading of the consignment without allowing access for the delivery staff to other parts of the building;
- the external entrance(s) of the storage area must be locked if the internal door is open;
- the protection of the area must be enhanced by employing security guards, if the protection level of the assets justifies it;
- the simultaneous opening of the external entrance of the storage area and the internal doors must trigger an alarm;
- incoming goods must be inspected before they are moved from the storage area to their final place of use in view of the potential hazards;
- the incoming goods must be registered, if possible, already at the time when they arrive at the business site.

5.7.2. Equipment

5.7.2.1. Equipment siting and protection

The equipment must be positioned and its protection must be designed in a way that minimises the risks that arise as a result of the environmental impacts and the risk of unauthorised access.

The protective measures facilitate the reduction of failures attributable to various environmental impacts. For this reason:

- the equipment must be positioned in way that minimises the unnecessary entries to the related work areas;
- the screens of the equipment and workstations storing and processing sensitive data must be positioned in a way that ensures that during their use no unauthorised persons can see the data displayed on the screen;
- the equipment requiring special protection must be isolated;
- measures should be taken to minimise the risks caused by theft, fire, explosives, smoke, water (or breakdown of water supply), fog, vibration, chemical impacts, disturbance in the power supply or electromagnetic radiation;
- eating, drinking or smoking in the immediate vicinity of the data processing equipment must be prohibited;
- the environmental conditions must be permanently monitored to recognise the situations which may have negative impact on the operation of the data processing equipment;
- the buildings accommodating the data processing equipment must be equipped with protection against lightning, while the electric power supply and the communication lines must be equipped with filters against high-frequency interference;
- the fire protection regulations must be observed;
- it is prohibited to bring any chemical substances or explosives, other than the standard household chemical substances and detergents, in all territories of CETIN Hungary.

5.7.2.2. Supporting utilities

The equipment must be provided with proper protection for the event of power outage or other electric irregularities.

The continuous power supply of the data processing equipment belonging to the high availability category must be ensured by:

- uninterrupted power supply;
- multiplexer feed, and
- reserve power supply.

5.7.2.3. Cabling security

Electric and data lines must be properly protected against interruption and sabotage.

The following rules must be observed as a minimum:

- the electricity and telecommunication cables to the data processing system must be conducted underground, where possible, or supplied with alternative protection;
- the network cables must be protected from unauthorised tapping or damages by applying, for example, special protective tubes or avoiding the laying of cables in public areas;
- in order to avoid disturbances the telecommunication cables must be conducted separately from the heavy current cables;
- the track of the internal data network cables must be designated in a way to avoid leading through public areas and tapping in the outer areas;
- the equipment and cables must be clearly and visibly identified (labelled) to minimise the errors (e.g. erroneous connection of network equipment);
- in order to facilitate the fast elimination of errors and recovery, the connections must be documented and the documentation must be kept up to date;
- additional precautionary measures must be implemented for the sensitive and critical systems;
- shielded cables, lockable rooms and cabinets at the terminal nodes;
- redundant traffic control and transmission medium;
- use of fibre optic transmission medium;
- electromagnetic shielding of cables;
- restricting the access to the "patch" cabinets and rooms;
- monitoring for the connection of unauthorised devices and their prompt removal.

5.7.2.4. Equipment maintenance

In the interest of ongoing operation, the IT equipment used for CETIN Hungary services must be maintained regularly in accordance with the manufacturer's recommendations. The scheduling and the organisation of the maintenance are the responsibility of the leader of operation area concerned.

The completed maintenance works must be documented and approved by the head of the given area.

When the maintenance cannot be performed with the use of internal resources, the competent manager must initiate the hiring of an external party (subcontractor). During the maintenance the provisions of the relevant regulations must be observed; for this purpose the contract for services must be formulated accordingly.

5.7.2.5. Removal of assets

The use of the equipment outside the secure area must be limited to the required minimum. Mobile computers (notebooks, tablets, smartphones) that are centrally managed, equipped with appropriate protection measures and individually assigned to a responsible user are approved to be used outside of the secure area.

5.7.2.6. Security of equipment and assets off-premises

In respect of the equipment used off-premises of CETIN Hungary, the following considerations must be taken:

- storage devices removed from the facilities must not be left unattended in public and other physically unprotected areas. Portable computers must be transported, if possible, hidden in handbags;
- when designing the protection of the equipment the manufacturer's recommendation must be taken into account (e.g. in the case of protection against electromagnetic field);
- encryption of electronic storages with cryptographic methods.

The removal of storage devices containing sensitive data for repair may only be done after erasing the hard disk (workstation, printer, etc.). If that is not feasible the storage must be removed from the equipment.

5.7.2.7. Secure disposal or re-use of equipment

It must always be ensured that the data are erased from the data storage equipment before its destruction or recycling.

Upon destroying or recycling the data storage equipment:

- the data stored on it must be erased so that they cannot be restored or the storage must be made physically unfit for use;
- the deletion or destruction must be approved by the owner of the data stored on the data storage equipment;

The data must be erased so that they cannot be restored also in the case of computers handed over for decommissioning or destruction. If the destruction is carried out by an external employee or organisation, the confidentiality conditions must be stipulated separately in the contract between the entity performing the destruction and CETIN Hungary, and the contractor must guarantee the erasing of the data so that they cannot be restored, and also the full and unconditional confidentiality.

The proper erasing of the data is the responsibility of the ISO. The erasure of the data must be documented in minutes.

5.7.2.8. Unattended user equipment

- Users must lock their computer or log out if they leave their workplace even for a short time.
- If computers are to be left unattended for a longer period, users must log out from the operating system or shut the computer down.
- Time-locked, password protected screen savers must be used to lock unused workstations with a wait time set to no longer than 10 minutes.

5.7.2.9. Clear desk and clear screen policy

- All materials containing non-public data (including hard-copy materials and electronic media) must be removed from desks and stored in locked, secure places at the end of the day or when they are no longer used or the desk is left unattended. Media containing DS2 classification data must be stored in an environment under strengthened physical protection.
- Those installing displays must strive to make the angle from which screens can be seen as narrow as possible so that screen content could not be read by those occasionally walking by and especially not seen from outside the building or the

protected area. If that cannot be ensured through display arrangement, interior blinds or other measures such privacy-enhancing filtering screens must be used.

- Users must log out from each application, then shut the computer down when they are finished with a work session.
- Documents and printouts coming from printers, faxes, and copiers must be protected from access by unauthorized parties either by instructing users to immediately remove them from the machines or by only allowing printing to begin when the authorized user is physically present at the printer device.

5.8. Operations security

5.8.1. Operational procedures and responsibilities

The responsibilities related to the data processing equipment must be clearly defined and the operating procedures must be documented.

5.8.1.1. Documented operating procedures

The operational procedures must include detailed instructions related to the operation of the systems, covering the following items as a minimum:

a) data management and processing;

b) keeping the system secure, requiring the timely installation of all vendor-issued security patches as an integral part of the day-to-day operation;

c) backup copies, backup and restore procedures with appropriate testing;

d) scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times;

e) instructions for the management of faults and other exceptions that may arise during the execution of the task, including the restrictions regarding the use of the system programs;

f) the support contracts related to the case of unexpected operational and technical difficulties and to ensure vendor-issued security patches are always available;

g) instructions regarding the management of special output or outputs classified as confidential, including the secure procedures of outputs arising from the erroneous execution of the tasks;

h) recovery procedures applied upon the occurrence of errors;

i) rules governing the management of log data.

Support and version control contract must be concluded for all systems that are critical in business and security terms.

Registers must be kept of all components of the system. The register must contain the hardware and software configuration and location of the servers and workstations, as well as the name of the group in charge of the operation. A register must be kept of the installed software as well, the preparation and maintenance of which is the responsibility of the group commissioned with this in the given operational area. The register must be kept in a way that permits establishing the data serving the identification (e.g. software name, manufacturer, version number, application owner) and management (e.g. software key, capacity data) of the program.

The operational procedures must be approved by the IOL.

The ISO shall review the adequacy of the operational procedures important in terms of security during the system audits; the colleague in charge of the update of the given document or procedures updates it with the necessary modifications and repeatedly obtains the approval for the procedure.

5.8.1.2. Change management

Change management procedures must be elaborated for the regulated execution of the changes of data processing tools. The purpose of the change management procedure is to ensure that the changes executed on the systems important or critical in terms of business are carried out in a planned way, subject to prior management approval, with the generation of documentation in the proper quality and with minimum adverse impact on business processes. The data management systems must be configured in a way that ensures the generation of a log entry on the changes executed in the systems, which impact confidential data (e.g. personal data of the customer) and influence the functioning of the system.

During the implementation of the change management procedures the following aspects must be considered:

a) the major changes must be identified and logged in the Ticketing System.

b) the potential impacts of the major changes must be assessed;

c) the major changes must be tested in a non-production environment before they are implemented in production;

d) backout procedures or other ways to reverse changes must be documented;

e) the planned changes must be authorised via the regular approval procedure;

f) the impacted colleagues must be informed of all relevant details of the changes;

g) the procedures determining the interruption of failed changes and the persons responsible for the return from those;

h) risks related to the changes (that may arise from the fact that some of the above requirements are not met) must be managed and documented;

i) risks related to the lack of a particular change must also be documented and managed (i.e. what happens if the change is not implemented);

j) in addition to regular changes, rules for emergency changes must also be developed and documented, together with the necessary compensating controls that must be used in the case of emergency changes to mitigate the associated elevated risks.

The change management process, the mandatory steps and actors thereof, and the tasks of the actors must be defined in the Change Management Process document of CETIN Hungary. The maintenance and update of the document is the responsibility of the IOL.

5.8.1.3. Capacity management

To ensure the continuous operation of the business processes, all supporting information systems must be adequately protected against the exhaustion of computational resources (processing power, memory, disk, network bandwidth, etc) that may lead to their failure or incorrect operation.

The load of the system resources must be continuously monitored, and if the signs of overload can be detected or forecast at any system component, the competent head of the functional area of the organization of CETIN Hungary must be immediately notified to this effect.

The resource requirements must be defined for all existing and new systems. The determined availability level and efficiency of the systems must be maintained, and where necessary developed, through the continuous monitoring and fine-tuning of the load.

The capacity management procedures must ensure the timely detection of errors.

The capacity planning forecast of the data processing equipment must take account of the new business requirements and the trends that may be identified on the basis of all available data.

The above tasks belong to the responsibility of the IOL.

5.8.1.4. Separation of development, testing and operational environments

All non-production (e.g. development, testing) environments should be separated from the operational (production) environment within CETIN Hungary's network.

Separation means that any development or testing environment has to be implemented in separated microsegments. CETIN Hungary's zone modelling and microsegmentation have to be followed when creating testing or development environment.

The separation of a non-production environment from the production environment shall be considered sufficient only if it is guaranteed that any change implemented in the non-production environment, regardless of its layer, can have absolutely no impact on the operation of the production environment, or any other production system, nor any production data in the production environments.

Access methods of development and testing environments have to comply with the general access requirements.

To reduce the complexity of the testing or development environment some security architecture simplification can be accepted if approved by ISO. (e.g. test database can be implemented in yellow zone instead of green zone if the test database does not and will not contain any production data.)

Same security measures and policies have to be applied to testing and development environments as for production systems. (e.g. access control, antimalware, logging, security and IT monitoring, vulnerability management, incident management)

5.8.2. Controls against malware

For providing CETIN Hungary services in a secure way, all systems concerned in service delivery are must be protected against malicious code.

It is the responsibility of ISO to establish, maintain and operate proper defence against malicious code and to prepare Virus Protection Policy.

5.8.2.1. Requirements for protection system against malicious code

Systems used by CETIN Hungary must be equipped with controls that reduce the risk of introducing malicious software into the environment. Such controls must be planned and implemented commensurate with the risk.

In the network used for providing services of CETIN Hungary, three-level antimalware protection system shall be established:

- Defence on gateway-level (controlling traffic through network gateways)
- Defence on server-level

- Defence on client level

There shall be no device operated in network used for service delivery without active antimalware protection.

Exception devices, where antimalware can be omitted:

- Devices with purpose built firmware where installation of any antimalware solution is not possible
- Appliances with operating system where Vendor support is lost if any additional components are installed (in this case, compensating controls must be evaluated and where appropriate, implemented)
- Platforms that are less exposed to the introduction of malicious code during normal operation, such as Linux, UNIX based infrastructure servers. Such devices must nevertheless also be protected from malware using other methods (e.g. FIM, only installing software from authorized, clean sources, etc).

5.8.2.2. Requirements for Virus Protection Policy

Virus Protection Policy of CETIN Hungary must contain the following procedures:

- Procedures and rules for preventing malware infections and large-scale virus attacks;
- Procedures and duties in case of a suspected or confirmed malware infection or large-scale virus attack;
- Procedures for the handling of alarms generated by the antimalware system;
- Duties during virus attack;
- Procedure for terminating virus attack alarm;
- Procedure for recovery after a virus attack.

5.8.3. Backup

Regular backups must be taken of the business data and software. A background environment must be provided to ensure that the essential business data and software can be recovered in the event of a storage failure or the failure/destruction of the IT systems. The backup and the recovery procedures must be documented and regularly tested.

When designing the backup and recovery procedures the following items must be considered:

- The range of data subject to backup must be defined;
- The backup and recovery procedures must be documented;
- The backup methodology and frequency (full, differentiated, incremental) must be in line with the business and information security expectations towards the data subject to backup, take into account the expected RTO and RPO values determined by the business as well as the time needed for recovery in the case of a disaster;
- A copy of the backups must be stored in different premises (building) than where the backup was taken, and must be stored in a lockable cabinet or otherwise protected from unauthorized access (both physical and logical);
- The recoverability of the data and systems must be tested at least once a year, and after each major system modification. The purpose of this is to verify the feasibility of the recovery time specified before, as well as the completeness of the backup as well as the integrity of the backup data and the correct operation

of the underlying storage devices. The testing may be combined with other tasks, e.g. with the testing of the disaster recovery plans;

- Where the confidentiality of the business data requires so the data on the backup storages must be protected by encryption, with appropriate key management;
- Where the cyclic data backup does not facilitate the full recovery of a previous status, although this is prescribed by the law/regulation, a backup copy of the system data must be taken with the frequency prescribed by the law/regulation on write-protected storage and retained for the prescribed period;
- It must be ascertained that the backup copy was taken successfully, and any potential error must be addressed in due course; for this purpose the backup process must be logged;
- The backup logs must be regularly verified.

In order to ensure full recovery the backup procedures must also cover the application, database and operating system layers. The backup procedures must also contain the retention period and the archiving date of the data.

The backup system must be stored at a lockable place (cabinet and/or premises providing proper protection against unauthorised access) in premises equipped with adequate environmental protection including a fire extinguishing system and protection against ingress of water and dust, where the prescribed operating circumstances can be guaranteed (such as e.g. the uninterrupted power supply, temperature, relative humidity, etc).

The exact backup rules applicable to the IT systems and equipment of CETIN Hungary are included in the IT Operation Policy, the preparation of which is the responsibility of the IOL.

5.8.4. Logging and monitoring

5.8.4.1. Event logging

Information management systems must be configured in a manner that they create an accurate audit trail recording user activities, exceptional and information protection events with the proper content and in the proper format. Log files must be retained in order to monitor the access-control system and to investigate events occurring later on, and their content must be checked regularly.

Log files if applicable must contain the following information:

- user identifier that uniquely identifies the user responsible for the given event;
- identifier or exact location of the log sending device;
- network address and protocol used;
- exact date and time when the event occurred (it must be registered if logging uses UTC or local time, and reliability of the time stamps must be ensured by configuring systems to continuously synchronize system clocks to a reliable time source);
- event details;
- unique identifier of the network session.

The logging system needs to record events of the following types:

- minimum the following of user log-in and log-out events:
  - log-ins and log-outs;

- successful and unsuccessful attempts to access the system;
- of the attempts to access to objects or resources according to the system's documentation:
  - successful data access attempts;
  - unsuccessful data access attempts;
  - file access and the types thereof (read, modify, delete, change of access privileges);
  - access type (read, create, modify or delete) in the case of accessing confidential data (e.g. customer's personal details);
- system configuration changes with detailed information about the change;
- system start, shutdown and restart events;
- connecting / disconnecting I/O devices;
- use of privileged access levels and any action performed with elevated privileges together with who executed them;
- use of utility programs is limited and logged based on technological environment and job;
- alerts generated by the access control system;
- events related to the protection system;
- network alerts.

The implementation of the above criteria system is the responsibility of the IOL.

5.8.4.1.1. Processing (parsing) of log information

The frequency of log file processing is to be defined by system and event type in a way so that it allows timely reaction to any event occurrences. Furthermore, it also needs to be set to match the logging setup so that no audit data is lost due to an overflow or overwriting occurring in the log files.

Investigating and maintaining log file data requires proper tools and their documentation. The tools necessary for auditing security event log files in the system must allow selective investigation of one or more users' activities.

It is the IOL and the ISO's responsibility to ensure the availability of the tools required for log file processing.

5.8.4.2. Protection of log information

Log entries must be protected against unauthorised access or loss. In the case of electronic logs, this must be ensured through appropriate user access settings, while hard-copy logs must be stored locked away, with access granted only to properly authorised persons assigned with logging tasks, or checking / investigating log data.

Whenever a security incident occurs, event logs must contain all data necessary to perform any successive investigations:

- Therefore, event logs must be stored taking into account the following aspects:
  - log data must have a reliable, accurate time stamp,
  - log data must remain available without their integrity compromised throughout any retention period specified,

- it must be ensured that data cannot be modified in any way after their creation,
- regarding data confidentiality, unauthorised parties must not gain knowledge of the data.

- Data recorded in the log must be protected against unauthorised access.
- Data recorded in the log must not be edited or deleted manually.

The fact of accessing log data must also be recorded in the relevant logs. This has to include

- the identification of the person who accessed the log,
- access date and time,
- the purpose of accessing the log.

All information systems and applications must support central log collection from all system layers. Events must be sent to the log collection server nearly real-time.

The log file retention period needs to be defined based on the applicable laws, provisions and internal regulations. As a general rule, unless specified otherwise, the entire log file must remain accessible online for 90 days. The log file can be archived when that period is over. The online data file can only be deleted if it has been backed up or archived.

It is the responsibility of ISO to develop, and of IOL to implement the log files protection mechanisms.

5.8.4.3. Administrator and operator logs

System administrator activities must be monitored using an automatic monitoring system, which allows monitoring the activities at database, application and operating system levels.

The log information must be protected same as the other log information.

The escalation procedure to be followed in the case of incidents induced - or suspected to have been induced - by a system administrator must follow the same pattern as the general incident escalation procedure, with the only difference being that, initially, only the IOL and ISO can learn of that within the IT area.

5.8.4.4. Clock synchronization

To provide for a universal interpretation of the log files of various systems, automatic mechanisms must be in place to ensure that the system clocks of all devices are synchronized.

5.8.5. Control of operational software

For control of operational software prescriptions of 5.8.1.2 shall be followed.

5.8.6. Technical vulnerability management

5.8.6.1. Management of security vulnerabilities

Information must be obtained on a regular basis about the current vulnerabilities of the systems used by the company, and it must be used to investigate the organisation's exposure. Measures must be taken to reduce related risks to an acceptable level, as needed.

When identifying and fixing security vulnerabilities, the following process needs to be followed:

- Vulnerability management responsibilities must be determined for each specific job, covering at least the following:
  - Vulnerability monitoring;

- Collecting vulnerability-related risks;
- Patch installation;
- Coordination.

- A termination deadline must be set based on the risk level of the specific technical vulnerability;
- Following the identification of a vulnerability, its risk level and the required measure must be determined;
- Potential impact of vulnerabilities must be assessed while taking exposure into account. Vulnerability management must always start with systems whose failure poses a higher risk;
- The change management procedures or the security incident management procedures must be followed when implementing the measures;
- If a vulnerability can be fixed with a patch, the risks stemming from the patch installation and from the vulnerability itself must be compared;
- Patches must be examined and tested before installation in order to avoid severe side-effects;
- If there is no patch available to fix a vulnerability, other, compensating controls must be evaluated and if possible, implemented, such as:
  - stopping the service related to the given vulnerability;
  - modifying access rules or implementing new access controls (e.g. installing network access control, i.e. a firewall);
  - introducing more stringent control levels to detect and prevent any attacks;
  - raising awareness relating to vulnerabilities.
- All activities carried out while managing vulnerabilities must be documented;
- The efficiency of the vulnerability management process must be regularly reviewed and assessed.

It is the ILO's responsibility to ensure that all identified security vulnerabilities are adequately mitigated in all system components under his/her management.

It is the ISO's responsibility to design and manage vulnerability tests to independently verify the correct operation of the vulnerability management process.

5.8.6.2. Restriction on software installation.

It is the responsibility of IOL that in IT infrastructure only approved software can be istalled.

In order to avoid abuse of software installation rules number of system administrators allowed to install softwares shall be reduced to minimum.

5.8.7. Information system audit considerations

5.8.7.1. Information systems audit controls

Information system audits, including the checking of the operating system, must be designed to reduce the probability of business processes being interrupted to a minimum. For this reason:

- audit requirements must be discussed with IOL;

- the area covered by the audit must be agreed on and checked;
- only read access rights can be issued for the purposes of accessing the software and the data as part of the audit;
- any access rights other than read rights can only be granted to separated copies of the system files, and must be cancelled when the audit is over;
- the IT resources required for the carrying out the audit must be specified in advance and their availability must be ensured;
- requirements associated with special or supplementary processes must be defined and approved separately;
- all access must be monitored and logged;
- all procedures, requirements and responsibilities must be documented.

5.8.7.2. Protection of system audit tools

System audit tools (e.g. software and data files) must be protected against unauthorised access and modification. Audit tools and their data files must be isolated from systems, and must be stored at storage locations other than those used by users.

5.9. Communication security

5.9.1. Network security management

5.9.1.1. Network controls

Approving allowed connections and protocols between firewall security contexts are the responsibility of relevant ISR and must be recorded.

System administrators must keep up-to-date records on protocols approved for use via internal networks.

Network services and protocols which are not used or are deemed to be unnecessary during a review must be disabled.

Approved protocols shall be reduced to absolute minimum.

When connecting systems, the following rules must be observed:

- The ISO's approval is required for systems with different information security classifications.
- Insecure, unencrypted network connections are to be avoided whenever more secure, encrypted protocols are technically available.
- If unavoidable to send user authentication data (user identifier, password) then it must be forwarded in an encrypted form in computer network. Wherever possible authentication mechanisms should be used which avoid sending passwords across the network (e.g certificate based authentication) or one-time passwords should be used.

5.9.1.2. Security of network services

Users can be granted access only to those services that they have explicit access rights to. These access rights are approved by the Information Security Responsibles (ISR) and set by the network operation team.

5.9.1.3. Segregation in networks

Networks must be divided into well separable logical subnets to ensure the security of information systems. Data transfer between subnets must be filtered with firewalls and/or other approved network perimeter defense devices.

Firewalls must be configured to allow as far as possible only the secure protocols (e.g. instead of http https, instead of LDAP LDAPS, instead of Telnet SSH, instead of FTP sFTP etc.)

The following security context shall be segregated as a minimum:

- **Insecure security context** (all external networks outside of CETIN Hungary's network including the Internet itself, Customer and Partner networks)
- **Exposed security context** (other models often refer this az "DMZ" zone ot "Tranzit" zone; any traffic with external parties must be through proxies/reverse proxies deployed inside this security context)
- **Non-exposed security context** (services in this context are reachable for internal users directly but external users via L7 reverse proxies only, placed into Exposed context)
- **Secure security context** (even internal users must not reach directly e.g. database servers / data repositories placed within this security context, but using only middleware or application servers placed into Non-exposed security context)
- **Management security context** (used for devices montoring and managing the rest of the infrastructure, including security monitoring devices)

These subnets must be segregated by firewalls from each other.

Only within the listed above network security contexts it is allowed to segregate virtual subnets (VLANs) for different purposes / different systems.

Traffic is not allowed between security contexts which are not "adjacent" to each other. Traffic is allowed to be passed through only one-by-one from less secure context to more secure context and the other way around.

When two systems residing in different security context must be connected then preferably the system in more secure context should initiate and build-up the connection to the less secure context.

Traffic from Insecure contexts to inside zones shall be passed through proxy solutions (e.g. reverse proxies), traffic from inside towards Internet through web gateway solution.

The firewalls and proxy gateways must be set up by system administrators assigned with this responsibility by the NOL.

5.9.2. Information transfer

5.9.2.1. Information transfer policies and procedures

In order to protect the data exchange between the parties participating in the communication the data exchange processes and rules must be documented, which should contain the following requirements as a minimum:

- protective solutions and procedures against tapping, copying, modification, deliberate rerouting and destruction;
- solution for protection against malicious software (viruses);
- protection of the attached files transmitted during electronic communication;

- rules governing the use of electronic communication equipment;
- procedure for the use of printers, copiers, faxes, etc. to provide protection against unauthorised access;
- procedure for the use of wireless networks;
- encryption solutions to maintain the confidentiality, integrity and authenticity of the data;
- compliance with the international and local rules and laws, the prescribed data retention and deletion period, and procedures for the compliance with these;
- rules governing the use of electronic communication channels (e.g. e-mail, SFTP, social network sites, etc.);
- the responsibility of the employees, contractual partners and external parties.

5.9.2.2. Agreements on information transfer

The information exchange method (electronic or manual) between CETIN Hungary systems and external organizations (including other CETIN and other Telenor BUs), shall be included in inter-organizational agreements.

When defining the information security conditions of the agreements the following must be considered:

- management responsibility for the supervision, launch and receipt of the transmission;
- confidentiality agreements and in the case of personal data, data processing agreements and any additional documentations required by law (e.g. DPIA, etc)
- procedures related to the documentation of the sender, the transmission, the dispatch and the receipt;
- the rules governing the selection of parties involved in the transmission and the processing;
- responsibilities in case of loss of data;
- the use of the labelling system related to sensitive or critical data, based on which the data can be properly protected;
- defining the data and the software owner and responsibility to ensure data protection, software copyright and compliance;
- special cautionary measures for the protection of sensitive data, e.g. cryptographic keys.

The method and rules of the data exchange must be stipulated in the agreement concluded between the participating parties. It is the responsibility of the ISO to ensure that the contract contains the listed rules.

5.9.2.3. Electronic messaging

Rules governing electronic correspondence and Internet browsing:

- User accounts with elevated privileges (such as local administrator rights) must not be used for Internet browsing, e-mail correspondence or instant messaging.

- The protection requirements regarding the electronic mails and attachments correspond to the protection and classification of other documents;
- data classified as DS1 and DS2 must be always sent in encrypted form if sent outside of PPF Telco group (e.g. in zipped files using WinZip, protected by an adequately complex password). The applied password must not be identical with or similar to the internal network password. The mail must not contain the password in inferable form. The password must be forwarded independently of the e-mail. (e.g. in SMS);
- The Internet users should refrain from forwarding or downloading any material that serves no direct business objectives bearing in mind the access to the internet sites are monitored and logged; the ISO may restrict the access to sites that cannot be related to the work.
- The purpose of the corporate mailing system is to support work-related administration. The storage area per employee is limited;
- During the electronic correspondence the users can manage only their own mailbox, by default, and they do not see the mailboxes of others;
- The users must not use the identifier of others or false identification data;
- It is forbidden to forward mails automatically from the internal network to a public mailing (e.g. Gmail or Freemail) network;
- The public mail networks (e.g. Gmail, Freemail, etc.) must not be used for business communication;
- The content of the mailbox at work must not be forwarded automatically to an external e-mail; The mailing system must not be used for advertising (except on the dedicated official advertising forum) or political purposes, or for hindering the work of others;
- The setting of the corporate mailing client must not be modified; e.g. setting a Gmail, Freemail, etc. account in Outlook;

It is permitted to visit internet sites not related to the administration and to conduct private correspondence on the electronic mailing system of CETIN Hungary subject to due caution and self-control.

- The private correspondence and the use of the internet for private purposes must not have any adverse effect on the work of the given employee, the business of CETIN Hungary and the reputation of CETIN Hungary.
- Do not use (for private purposes) your company e-mail address:
  - for online registration (e.g. forum, etc.);
  - subscription to newsletters;
  - online shopping.
- During private correspondence the corporate employee/contractor data must not be used, with the exception of the business e-mail address.
- The corporate e-mail address must not be displayed on non-corporate (e.g. personal) web pages.
- The signature in the e-mail must follow the format accepted in CETIN Hungary.
- Activity that is offending others, hurting others' religious, ethnic, political or other type of sensitivity or insulting others is forbidden.

- The files belonging to the business activity or sphere of interest must not be taken out with the use of the Internet, or uploaded to external servers or shared in any way.

5.9.2.4. Confidentiality or non-disclosure agreements

All employees and external organisations, persons (company, individual employee, etc.) involved in CETIN Hungary service delivery must sign a confidentiality declaration, in which they represent that they shall not disclose the non-public data they learnt during their work to third parties either during or after the end of their work. The retention period applicable to confidential data is defined by ISO.

The periodic review of the Confidentiality Agreement (in local language and in English) and the modification thereof as necessary are the responsibility of the ISO.

5.10. System acquisition, development and maintenance

5.10.1. Security in development and support processes

5.10.1.1. System change control procedure

Only the explicitly appointed, competent systems administrators are authorised to install program products.

If it cannot be clearly determined if a new version properly interfaces with the existing tools, the core or the user systems, the SCOL has the right to decide on its future use.

To ensure processing security, all documentation must be kept up-to-date.

In order to reduce information system errors, always use strict control when implementing changes.

The following must be ensured in the course of the procedure:

- testing the change in a non-production environment with appropriate depth and coverage
- setting up user access levels;
- changes can only be proposed by authorised persons;
- full and complete implementation of precautions including rollback procedures;
- identifying all software, data, databases and hardware which are affected by the change;
- that the authorised user accept the changes before they are implemented;
- that the system documentation be updated in parallel to the implementation of each change, and old documents are archived and/or marked as obsolete;
- that all software upgrades be executed with change tracking;
- that every change request be logged;
- that the change does not result in the loss of previously available vendor support due to an unsupported configuration;
- that operation documentation and user procedures are fixed as necessary;
- that changes are introduced in time and without interfering with business processes.

It is the ISO's responsibility to set up and fulfil the requirements.

5.10.1.2. Technical review of applications after operating platform changes

Application systems must be checked after they are changed, and they must be tested for any operational damages and security breaches as follows:

- integrated precautionary functions must be checked and integrity checks must be performed to verify that the change implemented in the operating system did not compromise the application;
- the system functionality must be verified to ensure no regressions were introduced;
- it must be ensured that the annual maintenance plan and budget cover the costs of the checks and tests becoming necessary due to the change in the operating system;
- it must be ensured that changes to the operating system can undergo proper testing prior to their implementation;
- the appropriate modifications must also be reflected in the Business Continuity Plan.

The above tasks are assigned to the responsibilities of the IOL.

5.10.1.3. Restrictions on changes to software packages

Centrally managed application software accepted from developers must not be changed (exception is software patching related to technical vulnerabilities described in 5.8.6).

Under special circumstances, when a change is inevitable, any actions changing one or more software functions are subject to the prior written permission of the head of the competent professional area, the approval of the head of the operation area. Before implementing a change it must be clarified if:

- it has an impact on the operation of the security functions existing in the original version;
- the required change is available from the developer;
- the conditions applicable to version control (maintenance) change as a result.

The original software must be kept, and the change must be implemented on a clearly identified copy. All changes must be tested and documented.

Implementing version upgrades or any other software tuning requiring significant interference is subject to approval by the IOL. The SCOL is only allowed to do it when he has received the approval, and the fact of performing the task must be documented.

5.10.1.4. Secure system engineering principles

When starting to implement a new system or to modify an existing one, all risks related to the implementation must be identified (exception is software patching related to technical vulnerabilities described in 5.8.6).

It is the responsibility of the system owner to ensure that from planning phase of the project and during the whole process information security aspects were taken into account, and risk analysis has been performed prior to starting implementation.

It is the responsibility of the ISO to assess information security risks.

The supplier implementing new systems and modifying the existing ones for CETIN Hungary must adhere to all applicable local laws and comply with CETIN Hungary's policies while performing these tasks. The information security requirements and expectations associated with the given project must be also recorded.

The project organisation must agree on and develop the best way of managing information security risks with the ISO. If identified risks cannot be avoided, this risk management method can be either risk mitigating measures (risk reduction), passing the risks on to a third party (risk transfer), or undertaking the risks (risk acceptance).

New or modified systems must be tested prior to and immediately following system introduction, and the operation of the developed risk mitigating controls needs to be verified. Testing must also include a system security analysis.

5.10.1.5. Outsourced development

When software development is outsourced to a third-party company, ownership, use and license rights must be defined and laid down. The method, the form and the minimum duration of tracking must be laid down. The source code of the developed software must be appropriate commented, and it must be stipulated that it be handed over to CETIN Hungary upon every release. Alternatively, if the developer is unwilling to hand over the source code, it may also be deposited in the care of a notary public with an instruction to be released to CETIN Hungary in case of a force majeure, immediately and free of charge. In such a case, a requirement must also be made that the thus escrowed copy of the source code be continuously kept up to date. The access rights necessary for auditing development quality and functionality, as well as the criteria checked during the investigation preceding installation must also be laid down.

Related to outsourced software development, the following controls must be used:

- A licensing agreement must be made;
- The conditions of use and the intellectual property rights related to the source code must be clarified;
- Software deposit agreements for a scenario where the third party goes bankrupt or ceases the development of the solution;
- Security and quality requirements must be set out in a contract;
- Assurance measures employed by the developer to guarantee the integrity and secure operation of all developed applications must be documented;
- All software components delivered must be clearly identified, versioned and signed with a developer certificate to help verify integrity and authenticity;
- Audit licenses must be provided for in the contract to verify compliance with the quality requirements;
- The delivered code must be tested for containing malicious and/or Trojan codes before installation. The developer must certify in writing that any software components delivered are free from any malicious code.

5.10.1.6. System acceptance testing

The new or modified system must be verified to ensure it meets all:

- functional,
- security,
- physical,

- operational and administration,
- back-up and recovery,
- reporting,
- manageability,
- monitoring,
- legal compliance,
- industrial control,
- internal CETIN Hungary's regulation

requirements.

Tests must be done to determine if new hardware and software devices can be installed. These tests must be documented in test reports.

New systems are installed after all their delivery documents have been approved by the IOL.

5.10.2. Test data

The production and non-production environments must be kept separate also in terms of the data that is being stored and managed in them. As a general rule, for development and testing purposes, a synthetic data set is to be used.

Production data shall only be stored and managed in the production environment and should not be used for development or testing. Likewise, production data must not be polluted by introducing fake/testing data into the production environment.

Exceptions may be granted on a case-by-case basis by the ISO, after careful consideration of all circumstances, including the sensitivity of data, applicable laws and regulations, and the existence (or lack of) compensating controls such as data redaction, depersonalization, audit logging and review, etc.

Real data can be used for test purposes only after depersonalisation (synthetic/anonymised database).

The following measures must be taken as a minimum to protect test data:

- If testing is done with the live database, the same user access management and data protection processes must be introduced as those introduced for the live environment.
- The ISO's prior approval is required if live data are to be copied into the test systems;
- Live data must be immediately removed from test system when the tests are finished.
- All activities related to live data used for testing must be logged.

It is the SCOL's responsibility to make sure that these requirements have been fulfilled.

5.10.3. System acquisition, development and maintenance

5.10.3.1. Security requirements of information systems

The information security related requirements should be included in the requiremens for new information systems or enhancements to existing information systems.

In case of a new system, the information security requirements have to be identified and documented as early stage of the project or implementation as possible: at the system specification / design / planning phase.

If the solution, any applications or part of the applications of the new system requires sourcing of any components from 3rd party, the information security requirements have to be communicated during the sourcing process as early as possible.

The new system has to follow all technical requirements of CETIN Hungary:

- The architecture of the new systems has to follow CETIN Hungary's zone modelling with microsegmentation;
- The new system has to follow all policies required to satisfy business and security requirements of CETIN Hungary regarding availability, confidentiality and integrity;
- All type of access to the systems has to follow CETIN Hungary's policies;
  - Administrative level access to new servers has to be separated from user access and has to be monitored by a privileged access management solution;
  - Administrative access of applications has to be separated from normal user access (if this is not possible, ISO approval is required for the exception);
- The new system has to be integrated into IT monitoring system of CETIN Hungary, including the integration of its audit logs into the log management system of CETIN Hungary;
- The new system has to be integrated into the security monitoring process of CETIN Hungary;
- Operation of the system has to be properly designed according to CETIN Hungary's requirements;
- Servers and applications have to be hardened according to industry best practice guidelines (wherever available);
- The new system has to be part of the vulnerability management process of CETIN Hungary.

System architecture, security requirements and acceptance of the new system have to be reviewed by a security architect of CETIN Hungary and have to be approved by the ISO prior to go-live.

5.11. Supplier relationships

5.11.1. Information security in supplier relationships

5.11.1.1. Information security policy for supplier relationships

It must be ensured that the agreements concluded with external parties are performed at the service level specified in the contracts and in compliance with the information security rules.

The external parties must also observe all relevant security requirements as soon as provided with access to related data and property.

They must pay particular attention to the application of the provisions of this ISP.

When employing external parties, confidentiality agreements must be concluded. The conclusion of these confidentiality agreements is the responsibility of the person signing the contract, designated in CETIN Hungary as contact person for the external party.

5.11.1.2. Addressing security within supplier agreements

The contractual partners of CETIN Hungary participating in providing CETIN Hungary services must also apply proper security controls in order to protect the confidentiality and integrity of the used data and documents, and to avoid the deliberate or unintentional compromising of them.

A written agreement – Confidentiality agreement – must be concluded with the external parties that get in contact with the IT system or have an impact on information security, which contains or refers to all such information security requirements that ensure compliance with the ISP and the rules introduced in CETIN Hungary. Access for a third party to the IT system and data of CETIN Hungary may only be provided after familiarising them with the ISP and the related regulations and concluding the aforementioned confidentiality agreement.

The following items must be included in the agreement in respect of the external parties, if applicable:

- the information security requirements stipulated in the ISP and any additional requirements set forth in CETIN Hungary 's other regulations in terms of:
  - property protection,
  - data protection,
- restrictions applicable to the copying and disclosure of data,
- an access control agreement, which contains:
  - the permitted access methods,
  - the process of access right and privilege management,
  - clear mapping of the external party's representatives with the available IT services, including the rights and privileges regarding their use,
  - conditions applicable to the control of access mode,
- in respect of all services and products to be delivered:
  - description,
  - the level of the services to be delivered, and the criteria applicable to the acceptance of the services and products,
- the mutual obligation of the parties to the agreement,
- the liability regarding the legal materials, e.g. in respect of the data protections laws, with special regard to the different legislative system of the individual countries, if the agreement also concerns the cooperation of parties from different countries or of EU organisations,
- the protection of intellectual property rights and the transfer of copyright, as well as the protection of collective work,
- the conditions of control, and the definition of the reports on those,
- the right to audit the responsibilities stipulated in the contract, or the right to have further external parties perform the audits,
- the process of problem solving and dispute resolution – if possible – taking into account any unforeseeable events,
- the responsibility related to the installation and maintenance of the hardware and software,

- clear and defined change management process,
- the training of the users and system managers in respect of the introduced methods, procedures and security,
- measures regarding the reports, notifications and investigations of security incidents and security breaches,
- CETIN Hungary's right to suspend all access if a serious breach of trust by the supplier is reasonably suspected, and immediately terminate the contract if such a breach is confirmed, with the right to demand compensation from the supplier for all damages such a breach caused to CETIN Hungary or its customers,
- the fact that upon contract expiry or termination, the data assets of CETIN Hungary (be it physical or non-physical) must be returned or destroyed,
- conditions applicable to the involvement of additional subcontractors in the fulfilment of the contract; confidentiality agreements.

The access by external parties must be immediately blocked when the reason for access no longer exists, in the case of a security breach, or automatically upon the expiry of the contract, whichever happens first; this is the duty of the SCOL.

The requirements related to the security rules specified in the agreements concluded with third parties are defined by the ISO or Security Director. The stipulation of the requirements related to the defined security and the control thereof is the responsibility of the ISO.

5.11.1.3. Information and communication technology supply chain

The risks, originating from the operating procedures in which external parties are involved, threatening the data and data processing tools in service delivery, must be identified; appropriate and documented measures, approved in writing by the ISO, must be taken and enforced against these, before granting the access right.

All connections to the devices accessed, managed or diagnosed remotely by external parties over data transmission networks used for providing services must be approved and logged upon each access, and such sessions must be recorded, the setting of which is the responsibility of the NOL.

It is the responsibility of the contact person designated in CETIN Hungary to inform the ISO prior to concluding the contract, if the contract impacts customer data and information security. The identification of the information security risk related to external clients must be performed on the basis of CETIN Hungary's risk analysis methodology.

5.11.2. Supplier service delivery management

5.11.2.1. Monitoring and review of supplier services

The quality of the services provided by the external party must be monitored and in the framework of inspections it must be checked whether the security requirements and other rules stipulated in the contract are observed.

The service management relation established with the external party must cover the following:

- regular verification whether the service levels are in line with the provisions of the contract;
- regular verification of the settlement and confirmation of the services prepared by the external party, and organising regular meetings as required by the contract;

- the external party and CETIN Hungary must elaborate procedures in the framework of which the information security incidents are reviewed;
- the security log entries, the operation problems and errors arising during the activity of the external party must be regularly verified.

The services related to external parties are managed by responsible Director. The external party must provide sufficient resources to comply with the security and compliance requirements stipulated in the contract. If any shortcoming is detected it must be reported to ISO immediately and the client must be also informed; the shortcomings must be eliminated as soon as possible, of which a report must be sent to the ISO.

Suppliers that are either found to be in gross non-compliance with contractual requirements, or those that repeatedly violate CETIN Hungary's security regulations exposing CETIN Hungary to substantial information security or legal risk, are to be officially excluded from further bidding processes. If the severity of the violation warrants it, contracts with such suppliers must be terminated.

5.11.2.2. Managing changes to supplier services

For the management of the changes in the security measures – including also the regulations and procedures – required and introduced in the contract concluded with the external party, such procedures must be elaborated that take the criticality of the business processes and systems in due consideration and ensure the reassessment of the risks.

The management of the changes related to the external party is the responsibility of the responsible Director.

5.12. Information security incident management

5.12.1. Responsibilities and procedures

CETIN Hungary deliberately strives to minimise damages resulting from security events and incidents.

The organization should be prepared to handle information security incidents, and processes should be developed and documented in the Security Incident Management procedures that ISO is responsible for.

5.12.2. Reporting information security events

A reporting, response and escalation process known organisation-wise must be introduced to report and manage information security events. This process must clearly specify what constitutes a security event/incident, as well as what must be done when an information security event is detected.

Information security events must be reported via Service Management ticketing or Case Management system.

The reporting process must cover at least the following:

- Employees reporting security events must receive a reply concerning the reported events;
- It must describe the behaviour to be followed when the information security event occurs;
- It must contain all relevant information;

- The person who detected the event should not take measures on his own accord but report it via Service Management;
- The process to be followed if the security misuse was perpetrated by an employee, a contracted party or a third party.

Personal Data Breach type of incident has to be reported according to the published data breach process of CETIN Hungary.

5.12.3. Reporting information security weaknesses

All employees, contracted parties or third parties are obliged to immediately report any information security weaknesses they become aware of to prevent information security events.

Information security weaknesses must be reported via Service Manager ticketing system.

The employees, contracted parties and third parties must be aware that under no circumstances do they have the right to exploit or to try to exploit the discovered security deficiencies unless specifically authorized to do so in writing by the ISO.

5.12.4. Assessment of and decision on information security events

After their discovery, all events affecting information security must be reported with no delay to the Security Analyst Office. The Security Analysis Office must take all reported security incidents seriously, and all such reports must be recorded in the security incident database, even if they later are confirmed to have low or no security impact.

A documented procedure must be implemented to report, investigate and counteract information security events, which provides for:

- appropriate level documentation;
- feedback management;
- keeping the report confidential regarding the reporting party, if need be;
- initial assessment of severity;
- investigation of the events, collection and correlation of evidence;
- taking corrective actions including containment, mitigation and other actions and keeping a record of all steps taken.

According to the security incident management process, it must be considered whether the measure introduced can be expected to properly reduce the probability of the event, i.e. it can be considered to be final, or further measures are required.

5.12.5. Response to information security incidents

A process must be introduced to eliminate any information security incidents and deficiencies detected. The responsibilities of each party taking part in the process must be defined.

Process efficiency must be regularly checked and improved.

Corrective actions must be taken when an information security event occurs. Corrective actions can ensure that data protection problems could be solved in a fast and effective manner. With the systematic use of corrective actions we can achieve continuous improvement in data management.

Corrective actions are usually taken in the following situations:

- when an employee or an interested third party (contractor, principal, consultant, auditor, expert etc.) makes an information security report,
- one-off and repetitious problems,
- non-compliances of the system (audit report).

The corrective actions must identify the problem, identify the causes of the faults, and design and introduce measures to prevent their recurrence. The use of corrective measures must be documented and their effectiveness must be measured periodically.

5.12.6. Learning from information security incidents

It is the ISO's responsibility to assess the damage caused by information security incidents and to improve the existing data protection systems and processes based on the experience gained during information security events.

The ISO must develop an action plan to prevent the information security incident from recurring.

The ISO must give an account of the information security events and incidents, and the developed and executed action plans in the annual reports.

5.12.7. Collection of evidence

It is necessary to collect evidence in sufficient quantity, quality and of appropriate credibility relating to each information security incident, and to store it for the necessary period. This is the responsibility of the ISO.

The process introduced to collect evidence must ensure that all collected evidence:

- can be used as evidence at court;
- is strong, i.e. is of appropriate quality and complete.

Concerning the information systems, it must be ensured that the systems are capable of producing evidence in an appropriate quality and with proper information content.

Proper controls must be introduced to ensure the strength of the evidence in its production and storage periods and until the time when it is used.

The following must be taken into account in relation to producing evidence of appropriate strength:

- For hard-copy documents, it must be ensured that the original copies are stored in a secure manner. It must be recorded who found the document, where and when it was found, and the identity of the witness who was present when the document was found. The investigation must make it certain that the original copy was not tampered with.
- A copy must be made of every electronic computer data storage medium used as evidence. Each step of the copy-making process must be recorded and made in the presence of at least two witnesses (following a 4 eyes principle). Original copies must be stored in a secure place.

5.13. Information security aspects of business continuity management

5.13.1. Information security continuity

5.13.1.1. Planning information security continuity

A Business Continuity Plan must be developed and used to mitigate the negative consequences of the interruption in business activities, and also to protect critical business processes from the negative effects of failures and disasters.

A business continuity planning process covering the entire CETIN Hungary organisation must be implemented for the continuity and maintenance of business processes. Business continuity management includes the following key elements:

- it must be identified what risks are to be faced, taking into account the level and the effect of the threats, and including the identification and priority order of critical business processes;
- the 'Business Continuity Plan' must contain the remaining management steps as well;
- a person must be appointed as being responsible for coordinating business continuity management;
- as well as the continuity of information security while maintaining business continuity (i.e. the continuous maintenance of an acceptable level of information security controls even during the time of business continuity events and crises, while the organization works to restore normal operation).

5.13.1.2. Implementing information security continuity

A Business Continuity Plan (BCP) and a related Disaster Recovery Plan (DRP) must be prepared to maintain business operation and for the purposes of the timely recovery of critical business processes following a failure or an interruption. The Business Continuity Plan and the related Disaster Recovery Plan must specify:

- the possibilities under which the core activity (emergency operation) can continue;
- manual workarounds for automated processing processes;
- the possibility of a dynamic regrouping of information resources or complementing the system with spare units or any other workaround solution based on using the equipment of a third-party company;
- which systems have priority in case of a limited emergency processing scenario;
- the steps of switching over to temporary operation based on reserve (or third-party) equipment;
- the system of data back-up to be performed as a precondition of disaster recovery.

The Disaster Recovery Plan must contain accurately detailed instructions on the measures to be taken to resume normal or limited operation in case the computer centre is struck by disaster. In every step of the Disaster Recovery Plan, care must be taken to maintain the continuity of information security.

The Disaster Recovery Plan must contain the following:

- the target status to be resumed after a disaster;

- the definition of disaster events;
- the person or persons making the decision on whether to declare a disaster and responsible for initiating the process;
- the scope of the DRP;
- the preventive actions to be taken;
- how to prepare for responding to a disaster;
- actions to be taken when a disaster strikes (included information security actions to);
- DRP testing and maintenance.

The Disaster Recovery Plan must always be updated if there is a major change in the information infrastructure or in the information security infrastructure (e.g. when a new information system is implemented).

The document describing the emergency shut-down and restart sequences for the systems running in the computing centre must be prepared by the SCOL, is approved by IOL and must be stored in the computer room in one copy.

5.13.1.3. Verify, review and evaluate information security continuity

The testing plan for business continuity plans contains the method and the date and time of testing specific plan elements. Any of the following methods can be applied as necessary:

- discussing business recovery instructions assuming different faults;
- simulations (mainly for practising post-incident/-disaster procedures);
- testing technical recovery (to ensure that the information system can be recovered to its original state) if there is a test system available;
- recovery at a different location (the business process runs simultaneously with the recovery at a location different from the base location) if the necessary conditions are provided at the other location;
- testing information security controls;
- testing third-party services (to check if the contract for the given third-party services and products is complied with);
- full-scale tests (to check if the organisation, the staff, the equipment, the utilities and the processes can properly manage the interruptions).

The SCOL is responsible for the drawing up, testing and continuous maintenance of the Disaster Recovery Plan. Apart from all this, the SCOL must also ensure that the backups necessary for system recovery exist and are available.

Based on the implemented plans the system recovery must be regularly tested from the backups. The performing of the reload is the responsibility of the appointed operator.

5.13.2. Redundancies

It is also required to maintain information security during the design and implementation of technical recovery. In order to ensure this, ISO should be continuously involved in the development of Disaster Recovery plans.

5.14. Compliance

5.14.1. Compliance with legal and contractual requirements

When planning, operating and managing information systems, all civil and criminal, judicial, regulatory and contractual obligations must be taken into consideration. The legal unit provides support for completing the above tasks.

5.14.1.1. Identification of applicable legislation and contractual requirements

When developing information systems, all legal, regulatory and contractual requirements relating to the given information systems must be determined and documented. All special precautions aimed at fulfilling the previous requirements as well as the responsibilities of individuals must also be defined and documented. The ISO's responsible to document the requirements.

5.14.1.2. Intellectual property rights

The procurement and use of protected software products must be controlled as follows:

- only properly licensed software products are allowed to be procured and operated;
- CETIN Hungary's employees must use only software which is properly licensed or acquired through an official procurement procedure and must not transfer it to anyone else;
- all certificates/vouchers proving the ownership of licenses, master disks, manuals etc. must be retained;
- the number of user licenses and the software inventory must be compared every time the software is installed to prevent that the number of installations exceed the allowed maximum number;
- installed software must be checked at least once a year to filter out any software that may have been installed without having the appropriate license. This must be detailed in a report;
- all stipulations and criteria pertaining to software and information downloaded from public networks must be fulfilled.

5.14.1.3. Protection of records

In accordance with legal, statutory, contractual and operational requirements, records must be protected from being lost, destroyed, accessed by unauthorised parties and against falsification. Retention times (as dictated by business, contractual or legal requirements) must be documented and records management processes must ensure that data are retained according to the documented retention requirements.

Concerning records Document Control Procedure must be taken into account.

5.14.1.4. Privacy and protection of personally identifiable information

All statutory requirements pertaining to the protection of personal data must be fully complied with.

The detailed regulation can be found in the Data Subject Rights Requests Handling.

5.14.1.5. Regulation of cryptographic controls

CETIN Hungary selects the cryptographic devices/tools used to protect category DS1 or DS2 data managed in its information system based on the requirements laid down by on its own internal requirements, as that selection is not set out by any legal requirement.

5.14.2. Information security reviews

5.14.2.1. Independent review of information security

The application of information security requirements must be annually audited by an expert (auditor) independent from either operation or development. This review is aimed at checking information security regularly and identifying any related deficiencies.

Information security internal audits must be carried out based on the instructions of the ISO. He must draw up an annual audit plan for conducting these audits. A record must be kept of the audits. Audit reports are drawn up by the ISO or his representative. The reports must identify the company requirements or internationally recognized industry standards and best practice frameworks serving as the basis for the audit.

It is the ISO's responsibility to make a proposal for eliminating the deficiencies found during internal audits. The implementation of the measures is checked by the ISO. An annual report must be drawn up about completing the checks.

5.14.2.2. Compliance with security policies and standards

The Security Director must regularly review the compliance of information processing and procedures.

Compliance audits held at least annually must cover the following areas:

- information systems including end user computing equipment, both on-premise and cloud-based;
- data asset owners;
- users (internal and external).

IT infrastructure operation’s employees take part in the regular review of compliance with Information Security Strategy, rules and all other security requirements their respective systems are affected by.

5.14.2.3. Technical compliance review

Technical compliance audits include checking if hardware and software protection procedures were properly implemented. This audit is carried out with the involvement of a specialist of this area. Checking can be done manually (using software tools if necessary) or automatically, by using an appropriate software package.

An expert of the given functional area must always be involved in the audit.

The compliance audit may include a vulnerability (intrusion) test, which requires approval by the ISO. Technical checking of CETIN Hungary's information system may only be carried out by a competent and properly authorised person, or under the supervision of such a person.

6. Final Provisions

Present policy is valid from issuing date until its recall.

7. Appendix

7.1. Asset Handling principles

See Asset_Handling.xlsx

7.2. List of Tables

7.3. List of Figures

No table of figures entries found.

7.4. References

[1] Key words for use in RFCs to Indicate Requirement Levels: https://www.ietf.org/rfc/rfc2119.txt