Decree 41/2015. (VII.15.) of the Minister of Interior

on the requirements relating to the technological security and secure information devices and products, and on the security classification and declaration of security levels determined in the Act L of 2013 on the information security of state and municipal bodies

On the basis of the authorization under Section 24 (2) *a)* of the Act L of 2013 on the information security of state and municipal bodies, acting within my function set out in points 5 and 20 of Section 21 of Government Decree 152/2014. (VI.6.) on the functions and powers of the members of the Government, in agreement with the Minister for National Development acting within his function set out in point 11 of Section 109 of Government Decree 152/2014. (VI.6.) on the functions and powers of the members of the Government,

I decree as follows:

Section 1 The body having electronic information systems being subject to the Act L of 2013 on the information security of state and municipal bodies (hereinafter referred to as 'Hungarian Cyber Security Act') shall classify its electronic information systems into security classes under the criteria set out in Annex 1.

Section 2 The body having electronic information systems or this body's organizational units under Section 9 (2) of the Hungarian Cyber Security Act (hereinafter referred to as 'Organizational Unit') shall determine the security levels pursuant to Annex 2.

Section 3 (1) Based on the classification carried out under Sections 1 and 2, the body having electronic information systems shall perform the requirements set out in Annex 3, related to the security class applicable to its electronic information systems as set out in Annex 4.

(2) If it is necessary to derogate from the administrative and physical security measures determined in regulations prepared under the provisions of this Decree regarding the body or the Organizational Unit having electronic information systems, due to a higher need for protection in case of an electronic information system, the derogations shall be recorded in the regulation of the electronic information system concerned, as prepared under the provisions of this Decree.

(3) If it is justified to determine a different security level regarding the Organizational Unit than the security level determined for the body, due to a higher need for protection determined for the body, the Organizational Units shall be classified separately as set out in Annex 2.

(4) If the body having electronic information systems operates or uses only certain elements or functions of the electronic information system in part or in full, the requirements set out in Annex 4 shall be fulfilled regarding these elements and functions.

(5) If the electronic information system is used by more bodies, the operator of the electronic information system shall fulfil the requirements necessary for the information security of the operation regarding all the bodies having electronic information systems which carry out tasks on an electronic information system.

(6) The operator of electronic information systems shall fulfil the requirements necessary for the information security of the operation regarding the bodies having electronic information systems, carrying out tasks on electronic information systems, that the compliance with the requirements shall be built in the policy related to information security of the bodies having electronic information systems. The operator of electronic information systems and the body having electronic information systems shall lay down the requirements necessary for the information security of the operation in the contract concluded for the operation of the electronic information system.

Section 4 This Decree shall enter into force on 16 July 2015.

Section 5[1]

Section 6 (1) If the body having electronic information systems classified its electronic information systems into security classes within the time limit set out in Section 26 of the Hungarian Cyber Security Act and fulfilled its notification obligation under Section 5 (1) *b)* and *c)* of the Decree of the Minister of Interior on the order of authority registration of the bodies subject to the Hungarian Cyber Security Act, the electronic information systems' classification under this Decree shall be performed in cases set out in Section 8 (1) of the Hungarian Cyber Security Act.

(2) If the body having electronic information systems determined the security level for the body within the time limit set out in Section 26 of the Hungarian Cyber Security Act and the security level does not change by applying provisions in Annex 2 of this Decree, moreover no Organizational Unit under Section 9 (2) of the Hungarian Cyber Security Act is designated and it fulfilled its notification obligation under Section 5 (1) *a)* of the Decree of the Minister of Interior on the order of authority registration of the bodies subject to the Hungarian Cyber Security Act, the body's classification under this Decree shall be performed in cases set out in Section 10 (5) of the Hungarian Cyber Security Act.

(3) If the development of electronic information systems is in progress at the entry into force of this Decree under the provisions of Decree 77/2013. (XII.19.) of the Minister for National Development on the requirements relating to the technological security and secure information devices and products, and to the security classification and declaration of security levels determined in the Act L of 2013 on the electronic information security of state and municipal bodies, the provisions of this Decree shall be applied from 1 October 2015 for this development of electronic information systems.

Section 7[2] This Decree serves the purpose of compliance with the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

---

[1] Repealed base on Section 12 of the Act CXXX of 2010. Ineffective from 17.07.2015

[2] Added by Section 14 of Decree 40/2017. (XII.29.) of the Minister of Interior. Effective from 10.05.2018

Annex 1 to Decree 41/2015. (VII.15.) of the Minister of Interior

Security classification of electronic information systems

1. General guidelines

1.1. When classifying the electronic information systems into security classes, the body concerned shall enforce the requirements of secrecy, integrity and availability of the data processed in electronic information systems regarding the functions of the systems and with corresponding weighting;

1.1.1. the requirement of integrity shall be highlighted in case of systems processing national data assets;

1.1.2. especially availability shall be required in case of critical information infrastructures;

1.1.3. the maintenance of secrecy shall be formulated as a basic need regarding sensitive personal data.

1.2. The security classification of electronic information systems is determined by the data processed in the electronic information system and the functions of the given electronic information system. The classification, which is approved by the head of the body, shall be carried out on the basis of a risk analysis. The National Cyber Security Authority may issue risk analysis methodologies as recommendations. If the body has no risk analysis methodology of its own, it shall apply the risk analysis methodology thus issued.

2. Security classes

2.1. The security classification set out in laws is the responsibility of the body concerned in accordance with the following principles. Points 2.2. to 2.6. serve only as a guideline for the decision:

2.2. In case of security class 1, only insignificant damage may occur, as

2.2.1. the electronic information system does not process data protected by laws (e.g. personal data);

2.2.2. there is no loss of confidence, the problem remains within the body concerned and can be tackled within there;

2.2.3. the direct and indirect material damage is insignificant compared to the budget of the body concerned;

2.3. In case of security class 2, minor damage may occur, as

2.3.1. personal data may be infringed;

2.3.2. it is of little value in terms of course of business or affairs of the body concerned, and/or only data or electronic information systems protected by internal (institutional) regulations may be infringed;

2.3.3. the possible societal-political impact may be handled within the body concerned;

2.3.4. the direct and indirect material damage amounts to 1% of the budget of the body concerned.

2.4. In case of security class 3, moderate damage may occur, as

2.4.1. sensitive personal data may be infringed, personal data may be infringed in large amounts;

2.4.2. in terms of course of business or affairs of the body concerned, electronic information systems managing sensitive processes or data constituting sensitive information or other data protected by laws (medical secret, legal professional privilege, insurance secret, bank secret, etc.) may be infringed;

2.4.3. the possible societal-political impact: there may be loss of confidence within the body concerned, or obligations set out in institutional regulations may be breached;

2.4.4. the direct and indirect material damage amounts to 5% of the budget of the body concerned.

2.5. In case of security class 4, big damage may occur, as

2.5.1. sensitive personal data may be infringed in large amounts;

2.5.2. the chance of personal injury may increase (including for instance discontinued care due to an incident, dangers due to the discontinued control of the system);

2.5.3. in terms of course of business or affairs of the body concerned, electronic information systems managing processes of high value, trade secrets or of particular sensitivity or data constituting such information may be infringed in massive amounts or significantly;

2.5.4. compliance with legislation or its implementation may fail, loss of confidence may occur within the body, personal liability shall be applied in the senior management or management of the body concerned as the possible societal-political impact of the damage;

2.5.5. the direct and indirect material damage amounts to 10% of the budget of the body concerned.

2.6. In case of security class 5, outstanding damage may occur, as

2.6.1. sensitive personal data may be infringed in particularly large amounts;

2.6.2. human lives are in imminent danger, personal injury may occur in large numbers;

2.6.3. the national data assets may be irreparably damaged;

2.6.4. the availability of a critical information system ensuring maintenance of operability of the country and the society is not ensured;

2.6.5. the possible societal-political impact: there may be sever loss of confidence against the body concerned, fundamental human rights or significant rights regarding the operation of the society may be infringed;

2.6.6. in terms of course of business or affairs of the body concerned, electronic information systems processing trade secrets of high value or extremely sensitive processes or data constituting such information may be infringed in massive amounts or significantly;

2.6.7. the direct and indirect material damage amounts to 15% of the budget of the body concerned.

Annex 2 to Decree 41/2015. (VII.15.) of the Minister of Interior

Determination of bodies and Organizational Units having electronic information systems, into security levels

1. The security level of the body concerned is level 1, if the body does not operate or develop an electronic information system, and neither involves other body or service provider (excluding telecommunications service providers) within its own competence. The means of technical data manipulation is not determined on its own, it does not make a technical or information technology decision regarding data processing, it has no decision-making power related to the development of the electronic information infrastructure used (excluding the location of IT system elements concerning the work-related activities of the body), it processes or technically manipulates individual pieces of data and information, and does not process critical data. The information security activity of the body covers primarily the regulation of the obligations related to information security of the persons coming into contact with electronic information systems and their accountability to the extent that the activity of the body or the persons may have impact on electronic information systems.

1.1. The requirements of the organizational security level 1s:

1.1.1. the body concerned shall ensure the work instructions, internal provisions, regulations concerning the information security being in force in the organizational area and in the area of the operation assigned to a task of the body, under point 1.1.3, or other documents for this purpose (hereinafter referred to as 'Regulation') to the relevant persons;

1.1.2. the continuous risk analyses procedure shall be the part of information security policies and rules, which shall contain built-in checkpoints;

1.1.3. the information security policy and rules may refer to the whole body and the area of its operation, or a definite asset or an Organizational Unit;

1.1.4. the information security policy and rules shall be approved by the manager entitled thereto according to the provisions applicable to the body;

1.1.5. the information security policy and rules shall contain the oversight system of information security, the obligations and responsibilities related to information security;

1.1.6. non-compliance with information the security policy and rules shall entail legal consequences.

2. The security level of the body concerned is level 2, if the body or the Organizational Unit uses such an electronic information system besides the characteristics of level 1, which processes personal data, and the body involves a service provider designated by laws.

2.1. The requirements of the organizational security level 2 in excess of the requirements of level 1:

2.1.1. the security control procedures of the body concerned shall be laid down in rules of procedures;

2.1.2. the rules of procedures under point 2.1.1. shall contain the process, the manner, the date, the executor, the subject, the means of implementation of control procedures;

2.1.3. each procedure shall clearly define information security responsibilities and security-conscious behaviour in regards to the persons getting in contact with electronic information systems, the information security officers and the Organizational Units;

2.1.4. each procedure shall be subject to the supervision of Organizational Units or persons, who are in direct contact with other persons or Organizational Units concerned by the procedure to implement the certain procedure;

2.1.5. the procedures and their implementation shall be documented in a manner that the control activity performed (including its features, in particular its depth, its personal and material scope) can be identified.

3. The security level of the body concerned is level 3, if the body or the Organizational Unit use, but does not operate an electronic information system supporting its professional tasks besides the characteristics of level 2. The body processes critical data, non-classified data, but not data of public interest or data accessible on public interest grounds; the body is a user of electronic information systems or a closed electronic information system operated centrally and protected by security solutions applicable to more bodies, and involves other external service providers for supporting its duties.

3.1. **The requirements of the organizational security level 3 in excess of the requirements of level 2:**

3.1.1. the body concerned involves the persons taking part in the security control procedures, and shall inform them about their duties and the expectations of them;

3.1.2. the procedures under point 3.1.1. shall be introduced regarding the body and the Organizational Units concerned in a regulated and verifiable manner, and it shall be made subject of education for the persons concerned;

3.1.3. the procedures under point 3.1.1. shall not be applied in individual or ad hoc procedures;

3.1.4. the procedures under point 3.1.1. shall be approved by the manager entitled thereto according to the provisions applicable to the body;

3.1.5. the operation under the predefined requirements of procedures shall be ensured by preliminary testing of the procedures under point 3.1.1.;

3.1.6. the body shall have information security cost-benefit analysis methodology.

4. The security level of the body concerned is level 4, if the body or the Organizational Unit operates or develops an electronic information system or a closed electronic information system besides the characteristics of level 3.

4.1. **The requirements of the organization security level 4 in excess of the requirements of level 3:**

4.1.1. the effectiveness and adequacy of information security measures of the operation and development shall be ensured by regular, predefined testing integrated in the operation or development activity;

4.1.2. the operation of all regulation procedure and control shall be ensured in a testing procedure according to the expected and predefined information security requirements;

4.1.3. immediate and effective, predefined security measures shall be introduced to respond to the detected or occurred security incidents, including but not limited to respond to the possible or occurred security incidents based on the notification of incident response centers, suppliers or other reliable sources, too;

4.1.4. the effectiveness and adequacy of the information security measures introduced for the security of each information, system or application shall be subject to embedded regular internal assessment, which internal assessment can be carried out either in whole or in part by subcontractors or other organization entitled thereto or supervising the body;

4.1.5. the embedded internal assessment of the body may not be substituted;

4.1.6. based on information related to potential or real security incidents derived from the source under point 4.1.3. and security, or based on warnings, testing procedures or security control shall be carried out;

4.1.7. the requirements defined on the basis of the assessment of testing (including but not limited to the requirements related to the type and frequency of testing, too) shall be documented, shall be approved by the person entitled and shall be introduced;

4.1.8. the frequency and depth of testing individual control procedure shall be adjusted to the security risk the inadequate operation of controls entail.

5. The security level of the body concerned is level 5, if the body or the Organizational Unit - besides the characteristics of level 4 - is an operator, a developer of the electronic information systems of infrastructures designated as European and national critical infrastructures under the Hungarian Critical Infrastructure Protection Act; or a body, an Organizational Unit entitled to implement information security controls, testing.

5.1. **The requirements of organization security level 5 in excess of the requirements of level 4:**

5.1.1. it shall be ensured that information security control procedures are embedded in the core activities of the body;

5.1.2. the continuous review and further development of regulations, testing procedures, security procedures shall be ensured;

5.1.3. the body shall have a comprehensive information security program, which is an integral part of the operation of the body and ensures raising the security awareness of the staff;

5.1.4. the staff of the body shall have information security operative capacity and expertise required for performance of tasks;

5.1.5. ability to detect and manage security vulnerabilities shall be implemented throughout the body;

5.1.6. the change of information security environment shall be monitored with continuous reassessment of threats and review of control procedures;

5.1.7. with regard to the external and internal environmental changes related to information security, further information security alternatives shall be defined;

5.1.8. the body shall create its own information security capability- and condition measurement and assessment methodology, shall define the indicators thereof and shall update it in case under point 5.1.7.

Annex 3 to Decree 41/2015. (VII.15.) of the Minister of Interior

1. Classification guidelines

1.1. General provisions

1.2. Security measures to be implemented and the sequence of their implementation shall be determined in the action plan created for achieving the desired security class (security level).

1.3. In the heading of 'Number', the number of the measures ordered to the certain number of the subtitle '*3. Security measure catalogue*' in Annex 4 is indicated.

1.4. Regarding the administrative and physical security measures, the security classes of electronic information systems of the body are shown by columns numbered 1 to 5.

1.5. During determining the requirements of logical security measures, point 2 of Annex 1 shall be taken into account, and the electronic information systems shall be classified into classes 2 to 5 according to information security principles (secrecy, integrity, availability). As security class 1 cannot be interpreted in the field of logical security measures, it is not included in the table.

1.6. In any of the columns,

1.6.1. '0' shows that the security measure indicated in the horizontal row is not compulsory in that security class;

1.6.2. 'X' shows that the security measure indicated in the horizontal row is compulsory in that security class.

2. Tables of classification of the security measures set out in subtitle "3. Security measure catalogue" of Annex 4:

A) 3.1. ADMINISTRATVE SECURITY MEASURES

	A	B	C	D	E	F	G
1.	**Number**	Type of the measure	Security class				
2.			**1**	2	3	4	5
3.	**3.1.1.**	**Core activities at organizational level**					
4.	3.1.1.1.	Information security policy and rules	X	X	X	X	X
5.	3.1.1.2.	Information security officer	X	X	X	X	X
6.	3.1.1.3.	Action plan and its milestones	0	X	X	X	X
7.	3.1.1.4.	Records of electronic information systems	X	X	X	X	X
8.	3.1.1.5.	Authorization process related to electronic cyber security	X	X	X	X	X
9.	**3.1.2.**	**Risk analysis**					
10.	3.1.2.1.	Risk analysis and risk management rules of procedure	X	X	X	X	X
11.	3.1.2.2.	Security classification	X	X	X	X	X
12.	3.1.2.3.	Risk analysis	X	X	X	X	X
13.	**3.1.3.**	**Procurement of systems and services**					
14.	3.1.3.1.	Rules of procurement procedure	0	0	X	X	X
15.	3.1.3.2.	Assessment of resources needs	0	0	X	X	X
16.	3.1.3.3.	Procurements	0	0	X	X	X
17.	3.1.3.3.2.	Enforcement of protection aspects during procurements	0	0	0	X	X
18.	3.1.3.3.3.	Design and implementation documentation of security measures	0	0	0	X	X
19.	3.1.3.3.4.	Functions - protocols – services	0	0	0	X	X
20.	3.1.3.4.	Documentation regarding electronic information systems	0	0	X	X	X
21.	3.1.3.5.	Security planning principles	0	0	0	X	X
22.	3.1.3.6.	Services of external electronic information systems	0	X	X	X	X

23.	3.1.3.7.	Independent evaluators	0	0	0	X	X
24.	3.1.3.8.	Continuous monitoring	0	0	X	X	X
25.	3.1.3.8.2.	Independent assessment	0	0	0	X	X
26.	**3.1.4.**	**Planning continuity of course of business (course of affairs)**					
27.	3.1.4.1.	Rules of procedure regarding continuity of course of business	0	X	X	X	X
28.	3.1.4.2.	Business continuity plan for IT resource outages	0	X	X	X	X
29.	3.1.4.2.2.	Consultation	0	0	0	X	X
30.	3.1.4.2.3.	Restart of core functions	0	0	0	X	X
31.	3.1.4.2.4.	Determination of critical system elements	0	0	0	X	X
32.	3.1.4.2.5.	Capacity planning	0	0	0	0	X
33.	3.1.4.2.6.	Restart of all functions	0	0	0	0	X
34.	3.1.4.2.7.	Continuity of core tasks and functions	0	0	0	0	X
35.	3.1.4.3.	Training to prepare for continuous operation	0	0	X	X	X
36.	3.1.4.3.2.	Simulation	0	0	0	0	X
37.	3.1.4.4.	Testing of business continuity plan	0	0	0	X	X
38.	3.1.4.4.2.	Coordination	0	0	0	X	X
39.	3.1.4.4.3.	Testing in backup processing site	0	0	0	X	X
40.	3.1.4.5.	Security storage location	0	0	0	X	X
41.	3.1.4.5.2.	Isolation of backup processing site	0	0	0	X	X
42.	3.1.4.5.3.	Business continuity availability	0	0	0	X	X
43.	3.1.4.5.4.	Business continuity restoration	0	0	0	0	X
44.	3.1.4.6.	Backup processing site	0	0	0	X	X
45.	3.1.4.6.2.	Isolation	0	0	0	0	X
46.	3.1.4.6.3.	Availability	0	0	0	0	X
47.	3.1.4.6.4.	Prioritizing services in backup processing site	0	0	0	0	X
48.	3.1.4.6.5.	Preparation for the start of operation	0	0	0	0	X
49.	3.1.4.7.	ICT services	0	0	0	X	X
50.	3.1.4.7.2.	Service priority provisions	0	0	0	X	X
51.	3.1.4.7.3.	Exclusion of joint possibilities of error	0	0	0	X	X
52.	3.1.4.8.	Backups of electronic information systems	0	X	X	X	X
53.	3.1.4.8.2.	Reliability and integrity test	0	0	0	X	X
54.	3.1.4.8.3.	Restoration test	0	0	0	0	X
55.	3.1.4.8.4.	Isolation of critical information	0	0	0	0	X
56.	3.1.4.8.5.	Alternative storage location	0	0	0	0	X
57.	3.1.4.9.	Restoration and restart of electronic information systems	0	X	X	X	X
58.	3.1.4.9.2.	Recovery of transactions	0	0	0	X	X
59.	3.1.4.9.3.	Recovery time	0	0	0	0	X
60.	**3.1.5.**	**Incident response**					
61.	3.1.5.1.	Procedure of incident response	0	0	X	X	X
62.	3.1.5. 2.	Automatic incident response	0	0	0	0	X
63.	3.1.5. 3.	Information correlation	0	0	0	0	X
64.	3.1.5.4.	Observation of security incidents	0	0	X	X	X
65.	3.1.5.5.	Automatic monitoring, data collection and examination	0	0	0	0	X
66.	3.1.5.6.	Notification of security incidents	0	0	X	X	X
67.	3.1.5.6.2	Automated report	0	0	0	X	X
68.	3.1.5.7.	Support for incident response	0	0	X	X	X
69.	3.1.5.7.2.	Automated support	0	0	0	X	X
70.	3.1.5.8.	Incident response plan	0	0	X	X	X
71.	3.1.5.9.	Training for incident response	0	0	X	X	X
72.	3.1.5.9.2.	Simulation	0	0	0	0	X
73.	3.1.5.9.3.	Automated training environment	0	0	0	0	X
74.	3.1.5.9.4	Testing of incident response	0	0	0	X	X

75.	3.1.5.9.4.2.	Consultation	0	0	0	X	X
76.	**3.1.6.**	**Security taking into account human factors (personal security)**					
77.	3.1.6.1.	Personal security rules of procedure	0	0	X	X	X
78.	3.1.6.2.	Security classification of positions and tasks	0	0	X	X	X
79.	3.1.6.3.	Inspection of persons	0	0	X	X	X
80.	3.1.6.4.	Procedure at the termination of a relationship	X	X	X	X	X
81.	3.1.6.5.	Handling reassignments, redirections and secondments	0	0	X	X	X
82.	3.1.6.6.	Requirements related to the (external) body having a contractual relationship with the body concerned	0	0	X	X	X
83.	3.1.6.7.	Disciplinary measures	X	X	X	X	X
84.	3.1.6.8	Internal consultation	0	0	X	X	X
85.	3.1.6.9.	Rules of conduct on the Internet	X	X	X	X	X
86.	**3.1.7.**	**Awareness and training**					
87.	3.1.7.1.	Contact with the organizational system determined in electronic information security laws and sectoral bodies serving this purpose	0	0	X	X	X
88.	3.1.7.2.	Training rules of procedure	X	X	X	X	X
89.	3.1.7.3.	Security awareness training	X	X	X	X	X
90.	3.1.7.4.	Internal threat	0	0	0	X	X
91.	3.1.7.5.	Role- or task-based security training	0	0	X	X	X
92.	3.1.7.6.	Documentation on security training	0	0	X	X	X

B) 3.2. PHYSICAL SECURITY MEASURES

	A	B	C	D	E	F	G
1.	**Number**	Type of the measure	Security class				
2.			**1**	2	3	4	5
3.	3.2.1.2.	Physical protection rules of procedure	0	X	X	X	X
4.	3.2.1.3.	Physical access permits	0	X	X	X	X
5.	3.2.1.4.	Physical access control	0	X	X	X	X
6.	3.2.1.4.2.	Access to the information system	0	0	0	0	X
7.	3.2.1.5.	Access to data transmission devices and channels	0	0	0	X	X
8.	3.2.1.6.	Access control of output devices	0	0	0	X	X
9.	3.2.1.7.	Monitoring physical access	0	0	X	X	X
10.	3.2.1.7.2.	Intrusion alerts, surveillance equipment	0	0	0	X	X
11.	3.2.1.7.3.	Monitoring access to electronic information systems	0	0	0	0	X
12.	3.2.1.8.	Checking visitors	0	0	X	X	X
13.	3.2.1.8.2.	Automated visitor information management	0	0	0	0	X
14.	3.2.1.9.	Power supply equipment and cabling	0	0	0	X	X
15.	3.2.1.9.1.	Backup power supply	0	0	0	X	X
16.	3.2.1.9.2.	Long-term backup power supply for the minimum expected operational capability	0	0	0	0	X
17.	3.2.1.10.	Emergency stop	0	0	0	X	X
18.	3.2.1.11.	Emergency lighting	0	0	X	X	X
19.	3.2.1.12.	Fire protection	0	0	X	X	X
20.	3.2.1.12.2.	Automatic fire suppression	0	0	0	X	X
21.	3.2.1.12.3.	Detection equipment, systems	0	0	0	0	X
22.	3.2.1.12.4.	Fire suppressing installations, systems	0	0	0	0	X
23.	3.2.1.13.	Temperature and humidity control	0	0	X	X	X
24.	3.2.1.14.	Protection against damage caused by water and other materials transported by pipeline	0	0	X	X	X
25.	3.2.1.14.2.	Automated protection	0	0	0	0	X

26.	3.2.1.15.	Supply and delivery	0	0	X	X	X
27.	3.2.1.16.	Location of electronic information system elements	0	0	0	X	X
28.	3.2.1.17.	Inspection	0	0	0	X	X
29.	3.2.1.18.	Delivery supervision	0	0	0	0	X
30.	3.2.1.19.	Maintenance staff	0	0	X	X	X
31.	3.2.1.19.2.	Maintenance with enhanced security measures	0	0	0	0	X
32.	3.2.1.19.3.	Timely repair	0	0	0	X	X

C) 3.3. LOGICAL SECURITY MEASURES

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1.	**Number**	**Type of the measures**	**Principles**											
2.			**Secrecy**				**Integrity**				**Availability**			
3.			**Security classes**											
4.			**2**	**3**	**4**	**5**	**2**	**3**	**4**	**5**	**2**	**3**	**4**	**5**
5.	**3.3.1.**	**General security measures**												
6.	3.3.1.3.	Connections of electronic information systems	0	X	X	X	0	X	X	X	0	X	X	X
7.	3.3.1.3.2.	Internal system connections	0	X	X	X	0	X	X	X	0	X	X	X
8.	3.3.1.3.3.	Restrictions on external connections	0	X	X	X	0	X	X	X	0	X	X	X
9.	3.3.1.4.	Safety of persons	X	X	X	X	X	X	X	X	X	X	X	X
10.	**3.3.2.**	**Planning**												
11.	3.3.2.1.	Security planning policy	0	0	X	X	0	0	X	X	0	0	X	X
12.	3.3.2.2.	System security plan	X	X	X	X	X	X	X	X	X	X	X	X
13.	3.3.2.3.	Action plan	X	X	X	X	X	X	X	X	0	0	0	0
14.	3.3.2.4.	Personal security	X	X	X	X	0	0	0	0	0	0	0	0
15.	3.3.2.5.	Information security architecture description	0	0	X	X	0	0	0	0	0	0	0	0
16.	**3.3.3.**	**System and service procurement**												
17.	3.3.3.2.	Development lifecycle of systems	X	X	X	X	0	0	0	0	0	0	0	0
18.	3.3.3.3.	Functions, ports, protocols, services	0	X	X	X	0	X	X	X	0	X	X	X
19.	3.3.3.4.	Developer change tracking	0	0	X	X	0	0	X	X	0	0	X	X
20.	3.3.3.5.	Developer security testing	0	0	X	X	0	0	X	X	0	0	X	X
21.	3.3.3.6	Development process, standards and devices	0	0	0	X	0	0	0	X	0	0	0	X
22.	3.3.3.7.	Developer education	0	0	0	X	0	0	0	0	0	0	0	0
23.	3.3.3.8.	Developer security architecture and design	0	0	0	X	0	0	0	X	0	0	0	X
24.	**3.3.4.**	**Security analysis**												
25.	3.3.4.1.	Security analysis rules of procedure	0	X	X	X	0	X	X	X	0	X	X	X
26.	3.3.4.2.	Security assessments	0	X	X	X	0	X	X	X	0	X	X	X
27.	3.3.4.3.	Special assessments	0	0	X	X	0	0	X	X	0	0	X	X
28.	3.3.4.4.	Measuring security performance	0	X	X	X	0	X	X	X	0	X	X	X
29.	**3.3.5.**	**Testing, training and supervision**												
30.	3.3.5.1.1.	Testing, training and supervisory procedures	0	X	X	X	0	X	X	X	0	X	X	X
31.	3.3.5.2.	Measuring security performance	0	X	X	X	0	X	X	X	0	X	X	X
32.	3.3.5.3.	Vulnerability test	0	X	X	X	0	X	X	X	0	X	X	X
33.	3.3.5.3.2.	Update capability	0	X	X	X	0	0	0	0	0	0	0	0
34.	3.3.5.3.3.	Update from time to time, before a new examination or after detection of a new vulnerability	0	X	X	X	0	0	0	0	0	0	0	0
35.	3.3.5.3.4.	Privileged access	0	X	X	X	0	X	X	X	0	X	X	X

36.	3.3.5.3.5.	Disclosable information	0	X	X	X	0	X	X	X	0	X	X	X
37.	**3.3.6.**	**Configuration management**												
38.	3.3.6.1.	Configuration management rules of procedure	X	X	X	X	X	X	X	X	X	X	X	X
39.	3.3.6.2.	Basic configuration	X	X	X	X	X	X	X	X	X	X	X	X
40.	3.3.6.2.2.	Reviews and updates	0	0	X	X	0	0	X	X	0	0	X	X
41.	3.3.6.2.3.	Preservation of previous configurations	0	0	X	X	0	0	X	X	0	0	X	X
42.	3.3.6.2.4.	Configuration of high-risk areas	0	0	X	X	0	0	X	X	0	0	X	X
43.	3.3.6.2.5.	Automatic support	0	0	0	X	0	0	0	X	0	0	0	X
44.	3.3.6.3.	Oversight of configuration changes (change management)	0	X	X	X	0	X	X	X	0	X	X	X
45.	3.3.6.3.2.	Preliminary testing and confirmation	0	0	X	X	0	0	X	X	0	X	X	X
46.	3.3.6.3.3.	Automatic support	0	0	0	X	0	0	0	X	0	0	0	X
47.	3.3.6.4.	Security impact assessment	0	X	X	X	0	X	X	X	0	X	X	X
48.	3.3.6.4.2.	Isolated test environment	0	0	0	X	0	0	0	X	0	0	0	X
49.	3.3.6.5.	Access restrictions regarding changes	0	0	0	0	0	0	X	X	0	0	0	0
50.	3.3.6.5.2.	Automatic support	0	0	0	0	0	0	0	X	0	0	0	0
51.	3.3.6.5.3.	Review	0	0	0	0	0	0	0	X	0	0	0	0
52.	3.3.6.5.4.	Signed elements	0	0	0	0	0	0	0	X	0	0	0	0
53.	3.3.6.6.	Configuration settings	0	X	X	X	0	X	X	X	0	X	X	X
54.	3.3.6.6.2.	Automatic support	0	0	0	X	0	0	0	X	0	0	0	X
55.	3.3.6.6.3.	Reaction to unauthorized changes	0	0	0	X	0	0	0	X	0	0	0	X
56.	3.3.6.7.	Narrowest functionality	0	X	X	X	0	X	X	X	0	X	X	X
57.	3.3.6.7.2.	Regular review	0	0	X	X	0	0	X	X	0	0	X	X
58.	3.3.6.7.3.	Non-executable software	0	0	X	X	0	0	X	X	0	0	X	X
59.	3.3.6.7.4.	Executable software	0	0	0	X	0	0	0	X	0	0	0	X
60.	3.3.6.8.	Electronic information system element inventory	X	X	X	X	X	X	X	X	X	X	X	X
61.	3.3.6.8.2.	Update	0	0	X	X	0	0	X	X	0	0	X	X
62.	3.3.6.8.3.	Automatic detection of unauthorized items	0	0	0	X	0	0	0	X	0	0	X	X
63.	3.3.6.8.4.	Protection against duplication	0	0	0	X	0	0	0	X	0	0	X	X
64.	3.3.6.8.5.	Automatic support	0	0	0	X	0	0	0	X	0	0	0	X
65.	3.3.6.8.6.	Logging	0	0	0	X	0	0	0	X	0	0	0	X
66.	3.3.6.9.	Configuration management plan	0	0	X	X	0	0	X	X	0	0	X	X
67.	3.3.6.10.	Restrictions on use of software	X	X	X	X	X	X	X	X	X	X	X	X
68.	3.3.6.11.	User-installed software	X	X	X	X	X	X	X	X	X	X	X	X
69.	**3.3.7.**	**Maintenance**												
70.	3.3.7.1.	System maintenance rules of procedure	0	0	0	0	X	X	X	X	X	X	X	X
71.	3.3.7.2.	Regular maintenance	0	0	0	0	X	X	X	X	X	X	X	X
72.	3.3.7.2.2.	Automatic support	0	0	0	0	0	0	0	X	0	0	0	X
73.	3.3.7.3.	Maintenance tools	0	0	0	0	0	0	X	X	0	0	X	X
74.	3.3.7.3.2.	Data carrier control	0	0	0	0	0	0	X	X	0	0	X	X
75.	3.3.7.4.	Remote maintenance	0	0	X	X	0	0	X	X	0	0	X	X
76.	3.3.7.4.2.	Documentation	0	0	0	X	0	0	0	X	0	0	0	X
77.	3.3.7.4.3.	Comparable security	0	0	0	X	0	0	0	X	0	0	0	X
78.	**3.3.8.**	**Data carrier protection**												
79.	3.3.8.1.	Data carrier protection rules of procedure	X	X	X	X	X	X	X	X	X	X	X	X
80.	3.3.8.2.	Access to data carriers	X	X	X	X	X	X	X	X	X	X	X	X

81.	3.3.8.3.	Labelling of data carriers	0	0	X	X	0	0	0	0	0	0	0	0
82.	3.3.8.4.	Storage of data carriers	0	0	X	X	0	0	0	0	0	0	0	0
83.	3.3.8.5.	Transport of data carriers	0	0	X	X	0	0	X	X	0	0	X	X
84.	3.3.8.5.2.	Cryptographic protection	0	0	X	X	0	0	X	X	0	0	0	0
85.	3.3.8.6.	Deletion of data carriers	X	X	X	X	0	0	0	0	0	0	0	0
86.	3.3.8.6.2.	Control	0	0	0	X	0	0	0	0	0	0	0	0
87.	3.3.8.6.3.	Testing	0	0	0	X	0	0	0	0	0	0	0	0
88.	3.3.8.6.4.	Deletion without destruction	0	0	0	X	0	0	0	0	0	0	0	0
89.	3.3.8.7.	Use of data carriers	X	X	X	X	X	X	X	X	X	X	X	X
90.	3.3.8.7.2.	Unknown owner	0	0	X	X	0	0	X	X	0	0	X	X
91.	**3.3.9.**	**Identification and authentication**												
92.	3.3.9.1.	Identification and authentication rules of procedure	X	X	X	X	X	X	X	X	X	X	X	X
93.	3.3.9.2.	Identification and authentication	X	X	X	X	X	X	X	X	X	X	X	X
94.	3.3.9.2.2.	Network access to privileged accounts	0	X	X	X	0	0	X	X	0	0	X	X
95.	3.3.9.2.3.	Network access to non-privileged accounts	0	0	X	X	0	0	X	X	0	0	X	X
96.	3.3.9.2.4.	Local access to privileged accounts	0	0	X	X	0	0	X	X	0	0	X	X
97.	3.3.9.2.5.	Replay protection	0	0	X	X	0	0	X	X	0	0	X	X
98.	3.3.9.2.6.	Remote access - separate device	0	0	X	X	0	0	X	X	0	0	X	X
99.	3.3.9.2.7.	Local access to non-privileged accounts	0	0	0	X	0	0	0	X	0	0	X	X
100.	3.3.9.2.8.	Replay-protected network access to non-privileged accounts	0	0	0	X	0	0	0	X	0	0	X	X
101.	3.3.9.3.	Device identification and authentication	0	0	X	X	0	0	X	X	0	0	X	X
102.	3.3.9.4.	Identities management	X	X	X	X	X	X	X	X	X	X	X	X
103.	3.3.9.5.	Management of authentication devices	X	X	X	X	X	X	X	X	X	X	X	X
104.	3.3.9.5.2.	Password-based (knowledge-based) authentication	0	0	X	X	0	0	X	X	0	0	X	X
105.	3.3.9.5.3.	Possession-based authentication	0	0	X	X	0	0	X	X	0	0	X	X
106.	3.3.9.5.4.	Inherence-based authentication	0	0	X	X	0	0	X	X	0	0	X	X
107.	3.3.9.5.5.	Registration personally or by a reliable third party	0	0	X	X	0	0	X	X	0	0	X	X
108.	3.3.9.6.	Feedback of the authentication device	X	X	X	X	X	X	X	X	X	X	X	X
109.	3.3.9.7.	Authentication for cryptographic module	0	X	X	X	0	X	X	X	0	X	X	X
110.	3.3.9.8.	Identification and authentication (users outside the body)	X	X	X	X	X	X	X	X	X	X	X	X
111.	3.3.9.8.2.	Accepting certificates of authentication service providers	0	X	X	X	X	X	X	X	X	X	X	X
112.	**3.3.10.**	**Access check**												
113.	3.3.10.1.	Access check rules of procedure	X	X	X	X	X	X	X	X	X	X	X	X
114.	3.3.10.2.	Managing user accounts	X	X	X	X	X	X	X	X	X	X	X	X
115.	3.3.10.2.2.	Automatic management	0	0	X	X	0	0	X	X	0	0	X	X
116.	3.3.10.2.3.	Removing temporary accounts	0	0	X	X	0	0	X	X	0	0	X	X
117.	3.3.10.2.4.	Disabling inactive accounts	0	0	X	X	0	0	X	X	0	0	X	X
118.	3.3.10.2.5.	Automatic logging	0	0	X	X	0	0	0	X	0	0	X	X
119.	3.3.10.2.6.	Logout	0	0	0	X	0	0	0	X	0	0	0	X
120.	3.3.10.2.7.	Unusual use	0	0	0	X	0	0	0	X	0	0	0	X
121.	3.3.10.2.8.	Disabling	0	0	0	X	0	0	0	X	0	0	0	X
122.	3.3.10.3.	Enforcement of access check	X	X	X	X	X	X	X	X	X	X	X	X

123.	3.3.10.4.	Enforcement of information flow control	0	0	X	X	0	0	X	X	0	0	X	X
124.	3.3.10.5.	Separation of responsibilities	0	0	X	X	0	0	X	X	0	0	X	X
125.	3.3.10.6.	Least privilege principle	0	0	X	X	0	0	X	X	0	0	X	X
126.	3.3.10.6.2.	Authorized access to security functions	0	0	X	X	0	0	X	X	0	0	X	X
127.	3.3.10.6.3.	Unprivileged access to security functions	0	0	X	X	0	0	X	X	0	0	X	X
128.	3.3.10.6.4.	Privileged accounts	0	0	X	X	0	0	X	X	0	0	X	X
129.	3.3.10.6.5.	Logging of the use of privileged functions	0	0	X	X	0	0	X	X	0	0	X	X
130.	3.3.10.6.6.	Blocking privileged functions for non-privileged users	0	0	X	X	0	0	X	X	0	0	X	X
131.	3.3.10.6.7.	Network access to privileged commands	0	0	0	X	0	0	0	X	0	0	0	X
132.	3.3.10.7.	Unsuccessful attempts to log-in	0	X	X	X	0	X	X	X	0	X	X	X
133.	3.3.10.8.	System usage indication	0	X	X	X	0	X	X	X	0	X	X	X
134.	3.3.10.9.	Simultaneous work phase management	0	0	0	X	0	0	0	X	0	0	0	X
135.	3.3.10.10.	Blocking of a work phase	0	0	X	X	0	0	X	X	0	0	X	X
136.	3.3.10.10.2.	Screen capture	0	0	X	X	0	0	X	X	0	0	X	X
137.	3.3.10.11.	Closing the work phase	0	0	X	X	0	0	X	X	0	0	X	X
138.	3.3.10.12.	Activities allowed without identification or authentication	X	X	X	X	X	X	X	X	X	X	X	X
139.	3.3.10.13.	Remote access	0	X	X	X	0	X	X	X	0	X	X	X
140.	3.3.10.13.2.	Control	0	0	X	X	0	0	X	X	0	0	X	X
141.	3.3.10.13.3.	Encryption	0	0	X	X	0	0	X	X	0	0	X	X
142.	3.3.10.13.4.	Access control points	0	0	X	X	0	0	X	X	0	0	X	X
143.	3.3.10.13.5.	Access to privileged commands	0	0	X	X	0	0	X	X	0	0	X	X
144.	3.3.10.14.	Wireless access	0	X	X	X	0	X	X	X	0	X	X	X
145.	3.3.10.14.2.	Authentication and encryption	0	0	0	X	0	0	0	X	0	0	0	X
146.	3.3.10.14.3.	Disabling user configuration	0	0	0	X	0	0	0	X	0	0	0	X
147.	3.3.10.14.4.	Antennas	0	0	0	X	0	0	0	X	0	0	0	X
148.	3.3.10.15.	Mobile device access control	0	X	X	X	0	X	X	X	0	X	X	X
149.	3.3.10.15.2.	Encryption	0	0	X	X	0	0	X	X	0	0	0	0
150.	3.3.10.16.	Use of external electronic information systems	X	X	X	X	X	X	X	X	X	X	X	X
151.	3.3.10.16.2.	Restricted use	0	0	X	X	0	0	X	X	0	0	X	X
152.	3.3.10.16.3.	Portable storage devices	0	0	X	X	0	0	X	X	0	0	X	X
153.	3.3.10.17.	Information sharing	0	0	X	X	0	0	0	0	0	0	0	0
154.	3.3.10.18.	Publicly available content	X	X	X	X	X	X	X	X	X	X	X	X
155.	**3.3.11.**	**System and information integrity**												
156.	3.3.11.2.	System and information integrity rules of procedure	0	0	0	0	X	X	X	X	0	0	0	0
157.	3.3.11.3.	Error correction	0	0	0	0	X	X	X	X	0	0	0	0
158.	3.3.11.3.2.	Automated error correction status	0	0	0	0	0	0	X	X	0	0	0	0
159.	3.3.11.3.3.	Central management	0	0	0	0	0	0	0	X	0	0	0	0
160.	3.3.11.4.	Malware protection	X	X	X	X	X	X	X	X	X	X	X	X
161.	3.3.11.4.2.	Central management	0	0	X	X	0	0	X	X	0	0	X	X
162.	3.3.11.4.3.	Automatic update	0	0	X	X	0	0	X	X	0	0	X	X
163.	3.3.11.5.	Supervision of electronic information systems	X	X	X	X	X	X	X	X	X	X	X	X
164.	3.3.11.5.2.	Automation	0	0	X	X	0	0	X	X	0	0	X	X
165.	3.3.11.5.3.	Supervision	0	0	X	X	0	0	X	X	0	0	X	X
166.	3.3.11.5.4.	Alerts	0	0	X	X	0	0	X	X	0	0	X	X

167.	3.3.11.6.	Security alerts and information	0	X	X	X	0	X	X	X	0	X	X	X
168.	3.3.11.6.2.	Automatic alerts	0	0	0	X	0	0	0	X	0	0	0	X
169.	3.3.11.7.	Checking security functionality	0	0	0	X	0	0	0	X	0	0	0	0
170.	3.3.11.8.	Software and information integrity	0	0	X	X	0	0	X	X	0	0	X	X
171.	3.3.11.8.2.	Integrity check	0	0	0	X	0	0	0	X	0	0	0	X
172.	3.3.11.8.3.	Detection and reaction	0	0	0	X	0	0	0	X	0	0	0	X
173.	3.3.11.8.4.	Automatic notification	0	0	0	X	0	0	0	X	0	0	0	X
174.	3.3.11.8.5.	Automatic reaction	0	0	0	X	0	0	0	X	0	0	0	X
175.	3.3.11.8.6.	Executable code	0	0	0	X	0	0	0	X	0	0	0	X
176.	3.3.11.9.	Protection against spams	0	0	0	0	0	0	X	X	0	0	0	0
177.	3.3.11.9.2.	Central management	0	0	0	0	0	0	X	X	0	0	0	0
178.	3.3.11.9.3.	Update	0	0	0	0	0	0	X	X	0	0	0	0
179.	3.3.11.10.	Input information check	0	0	0	0	0	0	X	X	0	0	0	0
180.	3.3.11.11.	Error management	0	0	0	0	0	0	X	X	0	0	0	0
181.	3.3.11.12.	Management and storage of output information	X	X	X	X	X	X	X	X	0	0	0	0
182.	3.3.11.13.	Memory protection	0	0	X	X	0	0	X	X	0	0	X	X
183.	**3.3.12.**	**Logging and accountability**												
184.	3.3.12.1.	Logging procedure	X	X	X	X	X	X	X	X	X	X	X	X
185.	3.3.12.2.	Events that can be logged	X	X	X	X	X	X	X	X	X	X	X	X
186.	3.3.12.2.2.	Review	0	0	0	X	0	0	0	X	0	0	0	X
187.	3.3.12.3.	Contents of log entries	X	X	X	X	X	X	X	X	X	X	X	X
188.	3.3.12.3.2.	Additional information	0	0	X	X	0	0	X	X	0	0	X	X
189.	3.3.12.3.3.	Central management	0	0	0	X	0	0	0	X	0	0	0	X
190.	3.3.12.4.	Log storage capacity	0	X	X	X	0	X	X	X	0	X	X	X
191.	3.3.12.5.	Logging error management	0	X	X	X	0	X	X	X	0	X	X	X
192.	3.3.12.5.2.	Logging storage check	0	0	0	X	0	0	0	X	0	0	0	X
193.	3.3.12.5.3.	Real-time alert	0	0	0	X	0	0	0	X	0	0	0	X
194.	3.3.12.6.	Logging investigation and reporting	0	X	X	X	0	X	X	X	0	X	X	X
195.	3.3.12.6.2.	Integration into processes	0	0	0	X	0	0	0	X	0	0	X	X
196.	3.3.12.6.3.	Summary	0	0	0	X	0	0	0	X	0	0	X	X
197.	3.3.12.6.4.	Integration of supervisory capabilities	0	0	0	X	0	0	0	X	0	0	0	X
198.	3.3.12.6.5.	Linking to physical access information	0	0	0	X	0	0	0	X	0	0	0	X
199.	3.3.12.7.	Log reduction and reporting	0	0	X	X	0	0	X	X	0	0	X	X
200.	3.3.12.7.2.	Automatic processing	0	0	X	X	0	0	X	X	0	0	X	X
201.	3.3.12.8.	Timestamps	X	X	X	X	X	X	X	X	X	X	X	X
202.	3.3.12.8.2.	Synchronization	0	0	X	X	0	0	X	X	0	0	X	X
203.	3.3.12.9.	Protecting log information	X	X	X	X	X	X	X	X	X	X	X	X
204.	3.3.12.9.2.	Restriction of access	0	0	0	0	0	0	0	X	0	0	X	X
205.	3.3.12.9.3.	Physically separate saving	0	0	0	0	0	0	0	X	0	0	0	X
206.	3.3.12.9.4.	Cryptographic protection	0	0	0	0	0	0	0	X	0	0	0	0
207.	3.3.12.10.	Non-repudiation	0	0	0	X	0	0	0	X	0	0	0	X
208.	3.3.12.11.	Preservation of log entries	X	X	X	X	X	X	X	X	X	X	X	X
209.	3.3.12.12.	Log generation	X	X	X	X	X	X	X	X	X	X	X	X
210.	3.3.12.12.2.	System-wide time-base log	0	0	0	X	0	0	0	X	0	0	0	X
211.	3.3.12.12.3.	Changes	0	0	0	X	0	0	0	X	0	0	0	X
212.	**3.3.13.**	**System and communication protection**												
213.	3.3.13.1.	System and communication protection procedures	X	X	X	X	X	X	X	X	X	X	X	X
214.	3.3.13.2.	Application separation	0	0	X	X	0	0	X	X	0	0	X	X
215.	3.3.13.3.	Separation of security functions	0	0	0	X	0	0	0	X	0	0	0	X
216.	3.3.13.4.	Residue information	0	0	X	X	0	0	0	0	0	0	0	0

217.	3.3.13.5.	Overload - service denial upon attack – protection	0	0	0	0	0	0	0	0	0	X	X	X
218.	3.3.13.6.	Border defences	X	X	X	X	X	X	X	X	X	X	X	X
219.	3.3.13.6.2.	Access points	0	0	0	X	0	0	0	X	0	0	X	X
220.	3.3.13.6.3.	External communication services	0	0	0	X	0	0	0	X	0	0	X	X
221.	3.3.13.6.4.	Default rejection	0	0	0	X	0	0	0	X	0	0	X	X
222.	3.3.13.6.5.	Disabling shared channel usage on remote devices	0	0	0	X	0	0	0	X	0	0	X	X
223.	3.3.13.6.6.	Authenticated proxy servers	0	0	0	X	0	0	0	X	0	0	0	X
224.	3.3.13.6.7.	Security error condition	0	0	0	X	0	0	0	X	0	0	0	X
225.	3.3.13.6.8.	Separation of system elements	0	0	0	X	0	0	0	X	0	0	0	X
226.	3.3.13.7.	Secrecy of data transmission	0	0	X	X	0	0	0	0	0	0	0	0
227.	3.3.13.7.2.	Cryptographic or other protection	0	0	X	X	0	0	0	0	0	0	0	0
228.	3.3.13.8.	Integrity of data transmission	0	0	0	0	0	0	X	X	0	0	0	0
229.	3.3.13.8.2.	Cryptographic or other protection	0	0	0	0	0	0	X	X	0	0	0	0
230.	3.3.13.9.	Disconnection of the network	0	0	0	0	0	0	0	0	0	0	X	X
231.	3.3.13.10.	Cryptographic key generation and management	X	X	X	X	X	X	X	X	X	X	X	X
232.	3.3.13.10.2.	Availability	0	0	0	X	0	0	0	X	0	0	0	X
233.	3.3.13.11.	Cryptographic protection	X	X	X	X	X	X	X	X	0	0	0	0
234.	3.3.13.12.	Collaborative IT devices	X	X	X	X	0	0	0	0	0	0	0	0
235.	3.3.13.13.	Public Key Infrastructure certificates	0	0	X	X	0	0	X	X	0	0	0	0
236.	3.3.13.14.	Mobile code restrictions	0	0	X	X	0	0	X	X	0	0	0	0
237.	3.3.13.15.	Voice over electronic information system (so-called Voice over Internet Protocol, VoIP)	0	0	X	X	0	0	0	0	0	0	0	0
238.	3.3.13.16.	Secure name / address resolution services (so-called authentic source)	0	0	0	0	0	X	X	X	0	0	0	0
239.	3.3.13.17.	Secure name / address resolution service (so-called resolution using recursive or cache storage)	0	0	0	0	0	X	X	X	0	0	0	0
240.	3.3.13.18.	Architecture and reserves for name / address resolution service	0	0	0	0	0	X	X	X	0	0	0	0
241.	3.3.13.19.	Authenticity of the work phase	0	0	0	0	0	0	X	X	0	0	0	0
242.	3.3.13.20.	Known condition after error	0	0	0	X	0	0	0	X	0	0	0	X
243.	3.3.13.21.	Residual information protection	0	0	X	X	0	0	X	X	0	0	0	0
244.	3.3.13.22.	Separation of processes	X	X	X	X	X	X	X	X	0	0	0	0

Annex 4 to Decree 41/2015. (VII.15.) of the Minister of Interior

ADMINISTRATIVE, PHYSICAL AND LOGICAL SECURITY REQUIREMENTS

1. DEROGATIONS

1.1. General requirements

The body may meet the minimal requirements determined in the security measure catalogue in point 3 with the possible derogations and measures in lieu, by choosing the measures appropriate to security risk level determined for the system, whilst every obligation applicable to the body shall be taken into consideration.

1.2. Individual derogations

1.2.1. Derogations regarding operation, environment:

1.2.1.1. The security measures depending on the nature of the operating environment shall only be applied, if electronic information systems are used in an environment making the measures necessary.

1.2.2. Derogations regarding physical infrastructure:

1.2.2.1. The security measures related to organizational facilities (locks, guards, environmental parameters: temperature, humidity, etc.) shall only be applied to the parts of the facilities that provide direct protection or security support for the electronic information system, or are related thereto (including the system elements, too, for instance e-mail, web servers, server farms, data centers, network hubs, border protection tools and communication equipment).

1.2.3. Derogations related to public access:

1.2.3.1. The security measures regarding public-accessible information shall be taken into consideration and implemented carefully, as certain security measures of the relevant part of security measure catalogue (e.g. identification and authentication, personal security measures) may not be applied to the users accessing through a public connection granted for the electronic information system.

1.2.4. Technological derogations:

1.2.4.1. The security measures regarding specific technology [e.g. wireless communication, cryptography, authentication procedure based on public key infrastructure (PKI)] shall only be applied, if these technologies are used in the electronic information system, or the use of them is prescribed.

1.2.4.2. The security measures concern only those components of the electronic information system which ensure or support the security capability targeted by the measure, and which are the sources of the potential risks intended to be reduced by the measure.

1.2.5. Derogations regarding security regulations:

1.2.5.1. When developing security measures applied for electronic information systems planned or already operating, the legal background determining the purpose of the system and also the functions shall be taken into consideration.

1.2.6. Derogations regarding gradual introduction of security measures:

1.2.6.1. Security measures may be gradually introduced. The gradation may be established on the basis of the security categorization of the electronic information systems to be protected.

1.2.7. Derogations regarding security purposes:

1.2.7.1. The security measures which exclusively support secrecy, integrity and availability may be reclassified (or modified, removed if not specified at a lower level of requirements) to a lower requirement level, if this lower level classification:

1.2.7.1.1. is in compliance with the requirement level determined before the application of the so-called 'high water mark' principle regarding the relevant secrecy, integrity and availability which principle means in the context of information security that all items must be tuned for the highest security purpose;

1.2.7.1.2. by applying the 'high water mark' principle, a higher security measure level exceeding the original secrecy, integrity and availability security purposes is determined, but this higher security measure level is not necessary from the perspective of cost-effective, risk-based security measures;

1.2.7.1.3. can be justified according to the risk analysis carried out for the body concerned;

1.2.7.1.4. shall have no impact on the important information relevant to security within electronic information systems.

1.2.7.2.[1] Regarding the electronic information system elements separated in a documented manner and independently assessed from IT security point of view, the security measures may be applied also separately with individual derogations following an examination set out in a risk analysis and risk management procedure adopted by the body, if border protection between separate elements was provided. The appropriateness of border protection as well as the reason and the extent of individual derogations shall be documented and shall be reviewed with a specified frequency.

2. ALTERNATIVE SECURITY MEASURES

2.1. The alternative security measure is a procedure which the body concerned intends to apply instead of the security measures for a given security class and which provides equivalent or comparable protection against the dangers forming real threat to the given electronic information system as well as ensures compliance with all external and internal requirements (e.g. acts or organizational regulations) in a manner equivalent to the replaced measure.

2.2. In case of an electronic information system, the body may apply alternative measures, if the following conditions are met:

2.2.1. if an alternative measure is chosen that can be found in security standards or national recommendations relevant to electronic information system security, or if there is no proper alternative measure in these documents, the body concerned may exceptionally apply an alternative measure that is appropriate in the given situation;

2.2.2. when choosing alternative measures, the body concerned shall endeavour to choose a measure from the security measure catalogue; the alternative measures determined by the body

[1] Added by Section 52 and point 1 Annex 4 of Decree 58/2016. (XII.22.) of the Minister of Interior. Effective from 01.01.2017

concerned may only be used as a last resort, if the security measure catalogue does not contain a measure applicable in the given circumstances;

2.2.3. it shall be presented in the relevant regulation how the alternative measures ensure equivalent security capabilities of the electronic information system, its security requirement level and why the security measures of the relevant basic set are not applicable;
2.2.4. the level of detail and rigor of the justification under point 2.2.3 shall be corresponding the security requirement level for the electronic information system;
2.2.5. if the body assesses and adopts the risk related to application of the alternative measure in accordance with the risk management procedures;
2.2.6. the application of alternative security measures shall be documented and shall be approved in accordance with the rules of procedure by the person or role concerned.

3. SECURITY MEASURE CATALOGUE

3.1. ADMINISTRATIV E SECURITY MEASURES

3.1.1. CORE TASKS AT ORGANIZATIONAL LEVEL

3.1.1.1. Information security policy and rules
3.1.1.1.1. The body concerned:
3.1.1.1.1.1. shall lay down information security policy and rules and shall document them according to requirements applicable to the body concerned, moreover it shall promulgate them within the body concerned;
3.1.1.1.1.2. shall determine the frequency of review and update of the information security policy and rules in another internal regulation or in the information security policy and rules themselves;
3.1.1.1.1.3. shall ensure that the information security policy and rules cannot be known or modified by unauthorized people.
3.1.1.1.2. In the information security policy and rules, the followings shall be ruled:
3.1.1.1.2.1. the purposes, the material and personal scope of the rules (its territorial scope depending on the nature of the body);
3.1.1.1.2.2. the roles related to electronic information security;
3.1.1.1.2.3. the activities assigned to the roles;
3.1.1.1.2.4. the responsibility related to the activities;
3.1.1.1.2.5. the internal cooperation of the information security organizational system.
3.1.1.1.3. The information security policy and rules shall primarily regulate the following fields related to information system security:
3.1.1.1.3.1. risk analysis (which closely links to the security classification and determination of security levels);
3.1.1.1.3.2. security situation and incident assessment procedure;
3.1.1.1.3.3. procurement of electronic information systems (including also their elements) and information technology service (if the body concerned carries out or may carry out such);

3.1.1.1.3.4. planning regarding security (for instance formation of procurement, development, rules of procedure);

3.1.1.1.3.5. rules of physical and environmental protection and its features;

3.1.1.1.3.6. prevention of threats to human resources (e.g. rules for staff recruitment and exit procedure, determination of personal commitments in labour contracts, enforcement of liability, etc.);

3.1.1.1.3.7. activities and trainings raising awareness on IT security regarding all workers, employees and agents standing in a public service or other employment relationship with the body concerned;

3.1.1.1.3.8. security setup tasks, expectations, rights related to electronic information systems applied at the body concerned (if it is applicable at the body concerned);

3.1.1.1.3.9. planning continuity of course of business, affairs or operation (in particular switching to manual procedures during system outage, return to the electronic system, generate missing data, etc.);

3.1.1.1.3.10. maintenance schedule of electronic information systems;

3.1.1.1.3.11. regulation of physical and logical protection of data carriers;

3.1.1.1.3.12. identification and authentication procedures applicable during access to electronic information systems, and monitoring compliance with access rules;

3.1.1.1.3.13. if the body concerned has the opportunity to do so, the assessment of system entries about the use of the systems, the determination of procedures depending on the result of the assessment;

3.1.1.1.3.14. the order of data saving and data archiving;

3.1.1.1.3.15. procedure at the occurrence of security incidents (including compromise of data, too), in particular the restoration;

3.1.1.1.3.16. requirements related to electronic information security and to be enforced during the conclusion of the contract which regulates the activities of non-members of the body concerned (maintenance workers, persons carrying out tasks to the body concerned based on private or civil law contracts) having access to the electronic information system (or physical access without authorization).

3.1.1.1.4. The information security policy and rules shall contain the expected security level of the body concerned and the expected security classes of every electronic information system of the body concerned.

3.1.1.2. Information security officer

3.1.1.2.1. The head of the body concerned shall appoint or entrust an information security officer who shall perform the duties determined in Section 13 of Act L of 2013 on the electronic information security of state and municipal bodies (hereinafter referred to as 'Hungarian Cyber Security Act').

3.1.1.3. Action plan and its milestones

3.1.1.3.1. The body concerned:

3.1.1.3.1.1. shall make an action plan, and determine milestone therein;

3.1.1.3.1.2. shall review and maintain the action plan at specified intervals:

3.1.1.3.1.2.1. on the basis of the risk management strategy and the priority of risk response activities;

3.1.1.3.1.2.2. if some deficiencies are found at the security classification regarding the given electronic information system, the review shall be carried out within 90 days after the test for the purpose of rectifying these deficiencies;

3.1.1.3.1.2.3. if the security level determined is lower than the level applicable to the body concerned, the review shall be carried out within 90 days after the test for the purpose of achieving the security level prescribed.

3.1.1.3.1.3. shall constantly update the records.

3.1.1.4. Records of electronic information systems

3.1.1.4.1. The body concerned:

3.1.1.4.1.1. shall keep a record on its electronic information systems;

3.1.1.4.1.2. shall constantly update the records.

3.1.1.4.2. The records shall contain the followings for all systems:

3.1.1.4.2.1. their core tasks;

3.1.1.4.2.2. the services to be provided by the systems;

3.1.1.4.2.3. the license numbers of the systems concerned (if they are processed by the body concerned);

3.1.1.4.2.4. identification and contact information of the person supervising the system;

3.1.1.4.2.5. identification and contact information of the system supplier, development and maintenance organizations, as well as identification and contact information of the contact persons competent in the system of these organizations.

3.1.1.5. Authorization process related to electronic information security

3.1.1.5.1. Authorization process related to electronic information security shall cover all:

3.1.1.5.1.1. the human, physical and logical resources;

3.1.1.5.1.2. the procedural and security requirement level and processes

falling within the scope of the body concerned.

3.1.2. RISK ANALYSIS

3.1.2.1. Risk analysis and risk management rules of procedure

3.1.2.1.1. The body concerned:

3.1.2.1.1.1. shall regulate risk analysis and risk management procedures and shall document them according to requirements applicable to the body concerned as well as shall promulgate them within the body concerned, which facilitates the implementation of risk analysis and risk management regulation and the controls related thereto;

3.1.2.1.1.2. shall determine the frequency of review and update of the risk analysis and risk management procedures in an internal regulation or in the document on risk analysis and risk management procedures itself.

3.1.2.1.2. The procedures shall cover:

3.1.2.1.2.1. the assessment of potential risks;

3.1.2.1.2.2. the responsibility for managing risks;

3.1.2.1.2.3. the expected quality of risk management.

3.1.2.2. Security classification

3.1.2.2.1. The body concerned:

3.1.2.2.1.1. shall examine its electronic information systems under the conditions laid down in laws, and shall determine based on the record under point 3.1.1.4 to which security classes they shall be classified;

3.1.2.2.1.2. shall approve the security classification by its manager;

3.1.2.2.1.3. shall set out the result of security classification in the information security policy and rules of the body.

3.1.2.2.2. Expectations:

3.1.2.2.2.1. security classification shall be repeated after changes concerning the electronic information systems;

3.1.2.2.2.2. connections shall be ensured to the action plan under point 3.1.1.3 and to its milestones.

3.1.2.3. Risk analysis

3.1.2.3.1. The body concerned:

3.1.2.3.1.1. shall perform security risk analyses;

3.1.2.3.1.2. shall record the result of risk analyses in the information security policy and rules, in the risk analysis report or in the document set out in risk analyses procedures;

3.1.2.3.1.3. shall review the result of risk analyses in compliance with the risk analyses procedures;

3.1.2.3.1.4. shall acquaint the persons concerned with the result of risk analyses in compliance with the risk analyses rules of procedure or in the framework of the information security policy and rules under point 3.1.1.1;

3.1.2.3.1.5. shall repeatedly perform risk analyses, if there is change in the electronic information system or in its operational environment (including but not limited to the emergence of new threats and vulnerabilities) as well as in circumstances that have an impact on security condition of electronic information system;

3.1.2.3.1.6. shall ensure that the result of risk analysis cannot be learnt by unauthorized persons.

3.1.3. PROCUREMENT OF SYSTEMS AND SERVICES

3.1.3.0. The procedures determined in this title shall not be introduced at the body concerned, if it does not procure IT services or devices in its own competence, and does not carry out or does not make system development activity carried out (excluding the typically low-value, commercially available, usually office applications, software or those hardware procurements which aim the replacement of damaged devices or expanding the equipment with the same or similar devices, as well as the procurement for repair, maintenance). For the purposes of this chapter, procurement and update of commercially available software does not constitute development.

3.1.3.1. Rules of procurement procedure

3.1.3.1.1. The body concerned:

3.1.3.1.1.1. shall regulate procurement rules of procedures and shall document them according to requirements applicable to the body concerned as well as shall promulgate them within the body concerned, which set out the rules for electronic information systems of the body concerned, for related procurement of services and information security system devices as well as facilitate the implementation of the controls related thereto;

3.1.3.1.1.2. shall review and update the rules of procurement procedures with a frequency determined in the rules of procurement procedures or in another internal regulation.

3.1.3.2. Assessment of resources needs

3.1.3.2.1. The body concerned:

3.1.3.2.1.1. shall determine, document and ensure the resources necessary for the protection of electronic information systems and their services for the purpose of performing the security requirements regarding electronic information systems and their services as a part of investment planning;

3.1.3.2.1.2. shall separately handle the security of electronic information systems in planning documents of the investment.

3.1.3.3. Procurements

3.1.3.3.1. The body concerned shall determine the followings in its procurement contracts for electronic information systems, system elements or services (including development, adaptation, procurement-related system monitoring or maintenance, too) as a contractual requirement:

3.1.3.3.1.1. the functional security requirements;

3.1.3.3.1.2. the warranty security requirements (e.g. the level of guarantee required for security-critical products);

3.1.3.3.1.3. the security-related documentation requirements;

3.1.3.3.1.4. the requirements for the protection of security-related documents;

3.1.3.3.1.5. specifications for the development environment and planned operating environment of the electronic information system.

3.1.3.3.2. Enforcement of protection aspects during procurements

The body concerned shall protect the electronic information systems, the system elements or the system services against the risks arising from the procurement or from the insertion of a procured equipment.

The body concerned shall prescribe for the developers, the suppliers as a contractual requirement, that they shall create and make the description of functional characteristics of the applicable security measures available.

3.1.3.3.3. Design and implementation documentation of security measures

The body concerned shall prescribe for the developers, the suppliers as a contractual requirement that they shall create and make the design and implementation documentation of applicable security measures available, including the description of the security-related external system interfaces, the low and high level security plan, and, if available to the supplier, the source code and the runtime environment.

3.1.3.3.4. Functions - protocols - services

The body concerned shall require from the developers, suppliers as a contractual provision that they shall determine functions, protocols and services designed for use already in the early stages of the development lifecycle.

3.1.3.4. Documentation regarding electronic information systems

3.1.3.4.1. The body concerned:

3.1.3.4.1.1. if it falls within its scope, shall require and take possession of the administrator documentation regarding electronic information systems, system elements or system services, which contains:

3.1.3.4.1.1.1. secure configuration, installation and operation of the system, system element or system service,

3.1.3.4.1.1.2. efficient application and maintenance of security functions,

3.1.3.4.1.1.3. vulnerabilities in the configuration and use of administrative functions that are known when the documentation is transferred;

3.1.3.4.1.2. shall require and take possession of user documentation regarding electronic information systems, system elements or system service, which contains:

3.1.3.4.1.2.1. the security functions available by users and their efficient methods of application,

3.1.3.4.1.2.2. the secure methods of use of the systems, system elements and system services,

3.1.3.4.1.2.3. the users' obligations for the maintenance of the security of systems, system elements and system services;

3.1.3.4.1.3. shall ensure that the documentation regarding the information systems (especially the administrator and developer documentation) cannot be learnt or modified by unauthorized persons;

3.1.3.4.1.4. shall ensure that the documentations shall be known by the persons holding specific roles determined by the body concerned or in accordance with the privileges of the role.

3.1.3.5. Security planning principles

The body concerned shall develop and apply security planning principles while defining, designing, developing, implementing and modifying the specifications of the electronic information system.

3.1.3.6. Services of external electronic information systems

3.1.3.6.1. The body concerned:

3.1.3.6.1.1. shall require as a contractual obligation that the services of electronic information systems used by it under a service contract shall comply with the electronic information security requirements of the body concerned;

3.1.3.6.1.2. shall determine and document the duties and obligations of users of the body concerned in relation with the services of external electronic information systems;

3.1.3.6.1.3. shall monitor with external and internal control tools, whether the service provider of the external electronic information system ensures the expected security measures.

3.1.3.7. Independent evaluators

The body shall employ independent evaluators or evaluator groups for assessing security measures.

3.1.3.8. Continuous monitoring

3.1.3.8.1. The body concerned shall carry out an embedded audit or an audit plan, which contains:

3.1.3.8.1.1. the area to be checked;

3.1.3.8.1.2. the audits and the frequency of assessments in support of audits;

3.1.3.8.1.3. ongoing security assessments in line with its audit strategy of the body concerned;

3.1.3.8.1.4. adequacy of metrics;

3.1.3.8.1.5. comparative analysis of security-related data generated by assessments and audits;

3.1.3.8.1.6. the reaction of the body concerned to the result of assessment of the security-related data;

3.1.3.8.1.7. the decision of the body concerned, on how often the analytical data shall be made available to the persons and roles defined thereby (including their changes, too).

3.1.3.8.2. Independent assessment

The body concerned may employ independent evaluators or evaluator groups for continuous monitoring of security measures of electronic information systems.

3.1.4. PLANNING CONTINUITY OF COURSE OF BUSINESS (COURSE OF AFFAIRS)

3.1.4.1. Rules of procedure regarding continuity of course of business

3.1.4.1.1. The body concerned:

3.1.4.1.1.1. shall regulate electronic information system rules of procedure and shall document them according to requirements applicable to the body concerned as well as shall promulgate them to the persons concerned within the body concerned, which facilitate the implementation of the regulation of the continuity of course of business and the monitoring related thereto;

3.1.4.1.1.2. shall review and update the rules of procedure for the continuity of course of business with a frequency determined in the business continuity plan or in another regulation.

3.1.4.2. Business continuity plan for IT resource outages

3.1.4.2.1. The body concerned:

3.1.4.2.1.1. shall regulate the business continuity plan for electronic information systems, and shall document it according to requirements applicable to the body concerned as well as shall promulgate it only to the persons and Organizational Units identified by name or role as key to continuous operation within the body concerned;

3.1.4.2.1.2. shall harmonize the activities regarding planning of continuous operation with incident response;

3.1.4.2.1.3. shall review the business continuity plan related to electronic information systems with a specified frequency;

3.1.4.2.1.4. shall update the business continuity plan in accordance with the changes of electronic information systems or operating environment as well as the problems arising during the implementation, enforcement or testing of the business continuity plan;

3.1.4.2.1.5. shall inform the key persons and Organizational Units identified by name or role as key to continuous operation about the changes of the business continuity plan;

3.1.4.2.1.6. shall ensure that the business continuity plan cannot be learnt or modified by unauthorized persons;

3.1.4.2.1.7. shall determine the core tasks (services to be provided) and core functions, as well as the emergency requirements related thereto;

3.1.4.2.1.8. shall decide about recovery tasks, recovery priorities and rates;

3.1.4.2.1.9. shall indicate the emergency roles, responsibilities and contact persons;

3.1.4.2.1.10. shall maintain the core services determined in advance by the body, even in the case of collapse, compromise or failure of the electronic information system;

3.1.4.2.1.11. shall develop the final recovery plan of the whole electronic information system, while not undermining the security protections originally planned and implemented.

3.1.4.2.2. Consultation

The business continuity plan shall be consulted with the Organizational Units responsible for related, similar plans.

3.1.4.2.3. Restart of core functions

The date of restart of the basic functions shall be determined following the activation of the business continuity plan.

3.1.4.2.4. Determination of critical system elements

The critical system elements supporting the core functions of the electronic information system shall be determined.

3.1.4.2.5. Capacity planning

The capacity required to ensure information processing, ICT and environmental skills necessary to continuous operation shall be planned.

3.1.4.2.6. Restart of all functions

The date of restart of all functions shall be determined following the activation of the business continuity plan.

3.1.4.2.7. Continuity of core tasks and functions

The continuity of core tasks and core functions shall be planned, so that no or only a small loss may occur in the operation continuity, and the continuity may be maintained until the complete restoration at the primary processing or storage place of the electronic information system.

3.1.4.3. Training to prepare for continuous operation

3.1.4.3.1. The body concerned shall hold trainings to users to prepare for continuous operation of electronic information systems in accordance with their roles and responsibilities:

3.1.4.3.1.1. within a specified period of time after they have taken on a role or responsibility;

3.1.4.3.1.2. with a specified frequency, or if changes in electronic information systems make it necessary.

3.1.4.3.2. Simulation

Simulated events shall be applied in the training for continuous operation to facilitate the efficient reaction of the staff in critical situations.

3.1.4.4. Testing of business continuity plan

3.1.4.4.1. The body concerned:

3.1.4.4.1.1. shall examine the business continuity plan regarding electronic information systems with a specified frequency and through defined tests in order to assess the effectiveness of the plan and the preparedness of the body concerned;

3.1.4.4.1.2. shall assess the testing results of the business continuity plan;

3.1.4.4.1.3. if necessary, shall improve the plan based on the assessment, and shall act concerning the improvement in compliance with the general procedural rules regarding business continuity plan.

3.1.4.4.2. Coordination

The testing of the business continuity plan shall be consulted with the Organizational Units responsible for related plans.

3.1.4.4.3. Testing in backup processing site

The business continuity plan shall be tested also in backup processing sites in order that the body concerned gets to know the features and available resources, as well as assesses the capacity of backup processing sites for supporting continuous operation.

3.1.4.5. Security storage location

3.1.4.5.1. The body concerned shall designate a security storage location, where the copies of electronic information system backups are stored in the same way and under security conditions as at the primary site.

3.1.4.5.2. Isolation of backup processing site

Backup processing site shall be isolated from the primary storage location for reducing sensitivity to the same hazards.

3.1.4.5.3. Business continuity availability

For the purpose of accessing the security storage location, emergency procedures shall be developed in the event of an area-wide destruction or disaster.

3.1.4.5.4. Business continuity restoration

The security storage location shall be established to facilitate recovery activities, in compliance with the purposes regarding recovery time and recovery points.

3.1.4.6. Backup processing site

3.1.4.6.1. The body concerned:

3.1.4.6.1.1. shall assign a backup processing site in order to - if the primary processing capability is not available to it - restart or continue the predefined operations of its electronic information system in the backup site within a predefined time, in compliance with the purposes regarding recovery time and recovery points;

3.1.4.6.1.2. shall ensure that the means and conditions necessary to restart or continue the operation shall be available in the backup processing site or within a predefined time;

3.1.4.6.1.3. shall ensure that the IT security measures of the backup processing site is equivalent to the measures applied at the primary site.

3.1.4.6.2. Isolation

A backup processing site shall be assigned which is separated from the primary processing site for reducing sensitivity to the same hazards.

3.1.4.6.3. Availability

For the purpose of accessing the backup processing site, emergency procedures shall be developed in the event of an area-wide destruction or disaster.

3.1.4.6.4. Prioritizing services in the backup processing site

Agreements shall be concluded and measures shall be introduced regarding the backup processing site, which contain service priority provisions in compliance with availability requirements of the body (inter alia recovery time purposes).

3.1.4.6.5. Preparation for the start of operation

The body concerned shall prepare the backup processing site that it shall be ready to use for supporting the operation of core functions within a defined time.

3.1.4.7. ICT services

3.1.4.7.1. The body concerned shall establish backup ICT services - with the exception of electronic information systems connected to the National Telecommunications Backbone Network -, in this regard it shall enter into such agreements which make the restart of core functions of an electronic information system or the restart of determined operations possible within a defined time, if the primary ICT capacity is available neither at the primary, nor the backup processing or storage sites.

3.1.4.7.2. Service priority provisions

If primary and backup ICT services are provided based on contracts, it shall contain service priority provisions in compliance with availability requirements of the body (inter alia recovery time purposes).

3.1.4.7.3. Exclusion of joint possibilities of error

Such backup ICT services shall be used, which reduce the probability of joint faults with the primary ICT services (e.g. are built on alternative technology).

3.1.4.8. Backups of electronic information systems

3.1.4.8.1. The body concerned:

3.1.4.8.1.1. shall perform saves about the user-level information stored in electronic information system with a specified frequency, in compliance with the purposes regarding recovery time and recovery points;

3.1.4.8.1.2. shall save the system-level information stored in electronic information system with a specified frequency, in compliance with the purposes regarding recovery time and recovery points;

3.1.4.8.1.3. shall save the documentation of the electronic information system (inter alia also the ones related to security) with a specified frequency, in compliance with the purposes regarding recovery time and recovery points;

3.1.4.8.1.4. shall protect secrecy, integrity and availability of the saved information both at the primary and the secondary storage site.

3.1.4.8.2. Reliability and integrity test

The saved information shall be tested with a specified frequency for guaranteeing reliability of data carriers and the integrity of information.

3.1.4.8.3. Restoration test

A selected sample shall be used from the security backup information at the restoration of selected functions of the electronic information system.

3.1.4.8.4. Isolation of critical information

Backup copies determined by the body concerned of the critical software of electronic information system and of other security-related information shall be stored on a separate equipment or in a qualified fireproof container.

3.1.4.8.5. Alternative storage location

Backup copy information of electronic information systems shall be stored in a security storage site determined in point 3.1.4.5.

3.1.4.9. Restoration and restart of electronic information systems

3.1.4.9.1. The body concerned shall ensure to restore the electronic information system to the last known state and to restart following a collapse, compromise, or failure.

3.1.4.9.2. Recovery of transactions

The body concerned shall carry out recovery of transactions in case of transaction-based electronic information systems.

3.1.4.9.3. Recovery time

The body concerned shall ensure the possibility that the electronic information system elements can be restored from a configuration-verified and integrity-protected information within a predefined time which represents the known operating status of the element.

3.1.5. INCIDENT RESPONSE

3.1.5.1. The body concerned:

3.1.5.1.1. shall develop incident response procedures which involve the preparation, detection, investigation, isolation, termination and recovery;

3.1.5.1.2. shall harmonize incident response procedures with the activities covering its business continuity plan;

3.1.5.1.3. shall incorporate lessons learnt from incident response activities to incident response procedures, development and operational procedures, expectations, continuous trainings and testing.

3.1.5.2. Automatic incident response

The body concerned shall apply automated mechanisms for supporting incident response procedures.

3.1.5.3. Information correlation

The body concerned shall link information regarding security incidents and reactions to individual events in order to gain organization-level insight to awareness related to security incidents and reactions.

3.1.5.4. Observation of security incidents

3.1.5.4.1. The body concerned shall monitor and document security incidents of electronic information systems.

3.1.5.5. Automatic monitoring, data collection and examination

The body concerned shall apply automated mechanisms in order to support monitoring of security incidents and collection, examination of information regarding security incidents.

3.1.5.6. Notification of security incidents

3.1.5.6.1. The body concerned:

3.1.5.6.1.1. shall require from everybody who is in contact with an electronic information system, or an object in which it is placed to report the occurrence of security incidents or if any indication or danger is detected;

3.1.5.6.1.2. shall report information regarding security incidents to authorities responsible for electronic information security supervision according to laws.

3.1.5.6.2. Automated report

The body concerned shall apply automated mechanisms in order to support the report of security incidents.

3.1.5.7. Support for incident response

3.1.5.7.1. The body concerned shall provide advice and support to users of electronic information systems for security incident response and report.

3.1.5.7.2. Automated support

The body concerned shall apply automated mechanisms in order to enhance availability of the information and support related to incident response.

3.1.5.8. Incident response plan

3.1.5.8.1. The body concerned:

3.1.5.8.1.1. shall develop security incident response plan which:

3.1.5.8.1.1.1. shall provide guidance about the methods of incident response to the body concerned,

3.1.5.8.1.1.2. shall describe the structure and organization of incident response opportunities,

3.1.5.8.1.1.3. shall provide a comprehensive approach to how incident response opportunities fit into the general organization,

3.1.5.8.1.1.4. shall meet individual needs related to the scope, size, organizational structure and functions of the body concerned,

3.1.5.8.1.1.5. shall determine notifiable security incidents,

3.1.5.8.1.1.6. shall determine and constantly refine the criteria of assessment and categorization (gravity, etc.) of security incidents,

3.1.5.8.1.1.7. shall provide support to internally measure security incident response opportunities,

3.1.5.8.1.1.8. shall determine the resources and leadership support which are necessary to expand, make more efficient and sustain security incident response opportunities;

3.1.5.8.1.2. shall announce the security incident response plan and have it acknowledged by the persons and Organizational Units handling security incidents (who are identified by name and/or role);

3.1.5.8.1.3. shall review security incident response plan with a specified frequency;

3.1.5.8.1.4. shall update the security incident response plan, taking into account the changes of electronic information systems and the body, or the issues arising during the implementation, enforcement and testing of the plan;

3.1.5.8.1.5. shall outline the changes in the security incident response plan pursuant to point 3.1.5.8.1.2;

3.1.5.8.1.6. shall ensure that the security incident response plan cannot be learnt or modified by unauthorized persons.

3.1.5.9. Training for incident response

3.1.5.9.1. The body concerned:

3.1.5.9.1.1. shall ensure security incident response trainings to the users of the electronic information system in compliance with the roles and responsibilities assigned to them;

3.1.5.9.1.2. the trainings shall be held within a specified time after the designation of the security incident response role or responsibility, or when the changes of electronic information system so require, or with a specified frequency.

3.1.5.9.2. Simulation

The body concerned shall apply simulated events in the security incident response training to facilitate the efficient reaction of the staff in critical situations.

3.1.5.9.3. Automated training environment

The body concerned shall apply automated mechanisms in order to ensure a deeper and more realistic environment for the security incident response training.

3.1.5.9.4 Testing of incident response

3.1.5.9.4.1. The body concerned shall test the security incident response capabilities regarding the electronic information system by using predesigned tests with a specified frequency in order to determine the effectiveness of security incident response and to document the results.

3.1.5.9.4.2. Consultation

The testing of security incident response shall be consulted with the Organizational Units responsible for related plans (e.g. business continuity plan and disaster response plan) by the body concerned.

3.1.5.9.5 Before their engagement, the persons involved in the investigation of security incidents shall take part in an information session about the security incident response procedure held by governmental incident response center.

3.1.6. SECURITY TAKING INTO ACCOUNT HUMAN FACTORS (PERSONAL SECURITY)

3.1.6.1. Personal security rules of procedure

Every personal security procedure or expectation shall cover the entire staff of the body concerned and all the natural persons who are or may be in contact with the electronic information systems of the body concerned. In cases where the person coming in actual or presumed contact with electronic information systems is not the member of the body concerned, the expectations in this chapter shall be enforced during the conclusion of the contract, agreement establishing the legal relationship forming the base of the activity as an obligation (including but not limited to commitments to getting to know and abiding by the regulations, rules of procedures as well as the confidentiality declaration).

3.1.6.2. Security classification of positions and tasks

3.1.6.2.1. The body concerned:

3.1.6.2.1.1. shall classify all relevant organizational positions or tasks related to the body concerned from a security point of view;

3.1.6.2.1.2. shall assess positions and tasks falling under an oversight of national security;

3.1.6.2.1.3. shall regularly review and update the security classification of positions and tasks.

3.1.6.3 Inspection of persons

3.1.6.3.1. The body concerned:

3.1.6.3.1.1. shall check before granting authorization to access the electronic information systems whether the person concerned meets the conditions for classification under points 3.1.6.2.1.1 and 3.1.6.2.1.2;

3.1.6.3.1.2. shall initiate the oversight of national security determined in National Security Services Act regarding the persons in the positions or performing the tasks under point 3.1.6.2.1.2;

3.1.6.3.1.3. shall monitor the existence of the terms under point 3.1.6.3.1 on an ongoing basis.

3.1.6.4 Procedure at the termination of relationship

3.1.6.4.1. The body concerned:

3.1.6.4.1.1. shall terminate the right to access the electronic information systems at a time specified in internal regulations;

3.1.6.4.1.2. shall terminate or withdraw the individual authentication devices of the person;

3.1.6.4.1.3. shall inform the person leaving about the relevant obligations surviving after the termination of the legal relationship which are legally enforceable as well;

3.1.6.4.1.4. shall withdraw all devices related to electronic information systems of the body which are owned by it;

3.1.6.4.1.5. shall retain the possibility of access to the electronic information systems and organizational information previously used, processed by the person leaving;

3.1.6.4.1.6. shall inform the persons performing the roles and tasks determined by it about the termination of the relationship in the manner specified by it;

3.1.6.4.1.7. shall ensure that the possible tasks of the person terminating the legal relationship related to the electronic information system or its security are performed, before the termination of legal relationship;

3.1.6.4.1.8. shall prevent such conduct of the person terminating the legal relationship that may possibly breach the electronic information security rules, affecting the electronic information system or the data stored therein at the termination of the legal relationship.

3.1.6.5 Handling reassignments, redirections and secondments

3.1.6.5.1. The body concerned:

3.1.6.5.1.1. shall, if necessary, carry out the procedure regarding the control of persons in point 3.1.6.3;

3.1.6.5.1.2. shall give authorization of logical and physical access to the electronic information system intended to be used newly;

3.1.6.5.1.3. shall, if necessary, carry out modification or termination of access permissions changed due to reassignment;

3.1.6.5.1.4. shall inform the persons performing the roles and tasks determined as sees fit about the change of relationship in the manner specified by it.

3.1.6.6. Requirements related to the (external) body having a contractual relationship with the body concerned

3.1.6.6.1. The body concerned:

3.1.6.6.1.1. shall require in the agreement, contract concluded with external bodies that the external body determines the roles and responsibilities concerning information security, related to the body concerned, including also the expectations regarding security roles and responsibilities;

3.1.6.6.1.2. shall require as a contractual obligation that the contracting party meets the personal security requirements determined by the body concerned;

3.1.6.6.1.3. shall require from the contracting party to document personal security requirements;

3.1.6.6.1.4. shall prescribe, that if a person quits from the contracting party or is reassigned who has authentication devices or exceptional privilege related to electronic information system of the body concerned, notification shall be sent to the body concerned out of turn;

3.1.6.6.1.5. shall monitor the compliance with personal security requirements of the contracting party on an ongoing basis.

3.1.6.7. Disciplinary measures

3.1.6.7.1. The body concerned:

3.1.6.7.1.1. shall initiate disciplinary proceedings against the persons breaching electronic information security rules and the rules of procedure related thereto, in accordance with its internal rules of procedure;

3.1.6.7.1.2. if the electronic information security rules are breached by a person not of the staff of the body concerned, it shall enforce the requirements determined in the relevant contract, shall examine the possibility of other legal action, and if necessary, shall introduce these procedures.

3.1.6.8. Internal consultation

The body concerned shall plan and consult the activities related to the security of electronic information systems to reduce their impacts on non-affected Organizational Units.

3.1.6.9. Rules of conduct on the Internet

3.1.6.9.1. The body concerned:

3.1.6.9.1.1. shall prohibit and account for illegal publication of information related to the body on public internet sites;

3.1.6.9.1.2. shall prohibit activities determined in internal regulations via Internet (e.g. chat, file exchange, non-professional downloads, forbidden sites, unwanted mailing lists, etc.);

3.1.6.9.1.3. may prohibit the use of social websites, access to a private mailbox and other activities foreign to the body.

3.1.7. AWARENESS AND TRAINING

3.1.7.1. Contact with the organizational system determined in electronic information security laws and sectoral bodies serving this purpose

3.1.7.1.1. The body concerned:

3.1.7.1.1.1. shall facilitate continuous education, training of the persons having access to electronic information systems;

3.1.7.1.1.2. shall keep the recommended electronic information security procedures, techniques and technologies up-to-date;

3.1.7.1.1.3. shall establish and maintain a contact for sharing latest information regarding threats, vulnerabilities and security incidents with the organizational system of electronic information security defined by laws and the sectoral bodies serving this purpose.

3.1.7.2. Training rules of procedure

3.1.7.2.1. The body concerned:

3.1.7.2.1.1. shall develop and document according to the requirements applicable to the body concerned, and promulgate the rules of training procedures within the body, which facilitates the implementation of the training regulations and the related monitoring;

3.1.7.2.1.2. shall review and update the training procedures with a frequency specified in the rules of training procedures or in other internal regulations.

3.1.7.3. Security awareness training

3.1.7.3.1. The body concerned shall provide awareness training about the fundamental security requirements to the users of electronic information systems:

3.1.7.3.1.1. as a part of the initial training of new users;

3.1.7.3.1.2. if changes in the electronic information system make it necessary;

3.1.7.3.1.3. with a frequency specified by the body concerned

in order that the persons concerned can be prepared for the detection of possible internal threats.

3.1.7.4. Internal threat

The security awareness training shall prepare the persons concerned for the detection of internal threats and shall raise awareness to their obligation of notification.

3.1.7.5. Role- or task-based security training

3.1.7.5.1. The body concerned shall provide role- or task-based security training to the persons in certain roles and responsible therefor:

3.1.7.5.1.1. before granting access to electronic information systems or implementing the tasks designated;

3.1.7.5.1.2. if changes in the electronic information system make it necessary;

3.1.7.5.1.3. with a frequency specified by the body concerned.

3.1.7.6. Documentation on security training

3.1.7.6.1. The body concerned:

3.1.7.6.1.1. shall document role- or task-based security trainings regarding security awareness;

3.1.7.6.1.2. shall make the completion of the training acknowledged by the persons taking part in the training and shall preserve the document.

3.2. PHYSICAL SECURITY MEASURES

3.2.1. PHYSICAL AND ENVIRONMENTAL PROTECTION

3.2.1.1. When applying this chapter, fire and personal protection provisions determined in other laws as well as provisions on personal data processing shall be taken into consideration, and also that the provisions of this chapter shall not be applied to the areas of the given facility that can be freely visited or used by anyone.

3.2.1.2. Physical protection rules of procedure

3.2.1.2.1. The body concerned:

3.2.1.2.1.1. shall develop and document according to the requirements applicable to the body concerned, and promulgate the rules of physical protection procedures applicable to the facilities or premises concerned by electronic information systems, which facilitates the implementation of the physical protection regulations incorporated in the electronic information security policy and rules or other regulations of the body concerned and the related controls;

3.2.1.2.1.2. shall review and update the rules of physical protection procedures with a frequency specified in the rules of physical protection procedures or in other internal regulations.

3.2.1.3. Physical access permits

3.2.1.3.1. The body concerned:

3.2.1.3.1.1. shall compile, approve and handle the list of persons authorized to enter the facilities where electronic information systems are located;

3.2.1.3.1.2. shall issue documents for the entry proving the right of entry (e.g. badges, ID cards, smart cards) to the persons intended to enter;

3.2.1.3.1.3. shall regularly review the list of persons authorized to enter;

3.2.1.3.1.4. removes those from the list of persons authorized to enter who are no longer eligible to enter;

3.2.1.3.1.5. shall take measures to withdraw, invalidate, delete, destroy the documents under point 3.2.1.3.1.2.

3.2.1.4. Physical access control

3.2.1.4.1. The body concerned:

3.2.1.4.1.1. shall ensure the physical entry of the authorized persons only at entry and exit points determined by the body concerned;

3.2.1.4.1.2. shall log physical entries;

3.2.1.4.1.3. shall keep the premises available to the authorized persons within the facility under control;

3.2.1.4.1.4. shall accompany the persons entitled to enter facilities ad hoc, and shall monitor their activities;

3.2.1.4.1.5. shall protect keys, access codes and other means of controlling physical access;

3.2.1.4.1.6. shall keep records about other means of controlling physical entries;

3.2.1.4.1.7. shall modify access codes and keys with a specified frequency or immediately, if the key is lost, the access code is compromised or the person loses its right to enter;

3.2.1.4.1.8. individual entry permits shall be controlled at entry points;

3.2.1.4.1.9. passing through designated points shall be controlled with a physical access control system or device determined by the body;

3.2.1.4.1.10. shall draw the attention of the members of the body to reporting abnormalities.

3.2.1.4.2. Access to the information system

Beyond the control of physical entries to the facility, the body concerned shall make physical entries in the premises of electronic information systems subject to a separate permit.

3.2.1.5. Access to data transmission devices and channels

The body concerned shall control physical entries in the premises of data transmission devices and connection points of electronic information systems, with security protection specified thereby.

3.2.1.6. Access control of output devices

The body concerned shall control physical access to output devices of electronic information systems in order to prevent unauthorized access.

3.2.1.7. Monitoring physical access

3.2.1.7.1. The body concerned:

3.2.1.7.1.1. shall control physical access in facilities of electronic information systems in order to detect physical security incidents and react to them;

3.2.1.7.1.2. shall regularly review the logs about physical accesses;

3.2.1.7.1.3. shall immediately review the logs about physical accesses, if information available indicates an unauthorized physical access;

3.2.1.7.1.4. shall harmonize the security incident responses with the result of log reviews.

3.2.1.7.2. Intrusion alerts, surveillance equipment

The body concerned shall supervise physical intrusion alerts and surveillance equipment.

3.2.1.7.3. Monitoring access to electronic information systems

Beyond the control of physical entries in the facility, the body concerned shall control the physical entries in the premises containing one or more parts of the electronic information system.

3.2.1.8. Checking visitors

3.2.1.8.1. The body concerned:

3.2.1.8.1.1. shall preserve the information about the visitors' entries in the facilities containing electronic information systems for a definite time;

3.2.1.8.1.2. shall immediately review the information and records about visitors' entries, if information available indicates an unauthorized access.

3.2.1.8.2. Automated visitor information management

The body concerned shall apply automated mechanisms to handle and review information and recordings about visitors' entries.

3.2.1.9. Power supply equipment and cabling

The body concerned shall protect power supply equipment of electronic information systems and cabling against injury and damage.

3.2.1.9.1. Backup power supply

In case of primary power outage, the body concerned shall provide a short-term uninterruptible power supply scaled to the activity, in order to shut down the electronic information system properly or to switch to long-term backup power supply.

3.2.1.9.2. Long-term backup power supply for the minimum expected operational capability

In case of primary power outage, the body concerned shall provide a long-term backup power supply to maintain the minimum expected operational capability and predefined minimum expected operating time of electronic information systems.

3.2.1.10. Emergency stop

3.2.1.10.1. The body concerned:

3.2.1.10.1.1. shall ensure possibilities to stop power supply of electronic information systems or individual system elements in emergency;

3.2.1.10.1.2. shall ensure safe and easy access to emergency stop equipment;

3.2.1.10.1.3. shall prevent unauthorized emergency shutdown.

3.2.1.11. Emergency lighting

The body concerned shall apply and maintain an automatic emergency lighting system which is activated in the event of a power outage and ensures emergency exits and escape routes.

3.2.1.12. Fire protection

3.2.1.12.1. The body concerned shall apply and maintain detection equipment with independent power supply for electronic information systems and fire suppression equipment suitable for IT equipment.

3.2.1.12.2. Automatic fire suppression

The body concerned shall apply automatic fire suppression capability for electronic information systems being not continuously supervised by staff.

3.2.1.12.3. Detection equipment, systems

The body concerned shall apply a fire alarm equipment or system for the protection of electronic information systems which activates automatically in the event of a fire and notifies the fire safety officer designated by the body concerned.

3.2.1.12.4. Fire suppressing systems, installations

The body concerned shall apply fire suppressing installations or system for the protection of electronic information systems about the activation of which the fire safety officer designated by the body concerned is notified automatically.

3.2.1.13. Temperature and humidity control

3.2.1.13.1. The body concerned:

3.2.1.13.1.1. shall maintain the temperature and humidity at the level required for the safe operation of resources in the premises where IT resources are concentrated (e.g. data center, server room, central engine room);

3.2.1.13.1.2. shall monitor the level of temperature and humidity in the premises where IT resources are concentrated (e.g. data center, server room, central engine room).

3.2.1.14. Protection against damage caused by water and other materials transported by pipeline

3.2.1.14.1. The body concerned:

3.2.1.14.1.1. shall protect electronic information systems against the damage from pipeline damage, ensuring that the main shut-off valves are available and operate properly as well as they are known by the key people;

3.2.1.14.1.2. shall ensure during designing the premises where IT resources are concentrated (e.g. data center, server room, central engine room) that they will be protected against water or other similar damage, even by replacing or relocating pipelines.

3.2.1.14.2. Automated protection

The body concerned shall apply automated mechanisms to detect fluid leakage near electronic information systems and to alert persons designated by the body concerned.

3.2.1.15. Supply and delivery

The body concerned shall permit or forbid, monitor and control the information system elements entering and leaving the facility and shall keep a record about them.

3.2.1.16. Location of electronic information system elements

The body concerned shall place electronic information system elements to minimize potential damage from physical and environmental hazards determined by the body concerned and to minimize the opportunity of unauthorized access.

3.2.1.17. Inspection

The body concerned shall inspect the maintenance equipment brought into the facility by maintenance staff for the purpose of preventing inappropriate or unauthorized modifications.

3.2.1.18. Delivery supervision

3.2.1.18.1. The body concerned shall protect the maintenance equipment containing information against unauthorized delivery whereby:

3.2.1.18.1.1. it shall inspect whether the equipment contains information;

3.2.1.18.1.2. if the equipment contains information, it shall be deleted or destroyed;

3.2.1.18.1.3. the equipment shall be preserved in the facility;

3.2.1.18.1.4. the delivery of the equipment shall be authorized by the persons responsible therefor.

3.2.1.19. Maintenance staff

3.2.1.19.1. The body concerned:

3.2.1.19.1.1. shall develop a procedure to manage the work permit of maintenance staff and shall keep a record about maintenance organization and persons;

3.2.1.19.1.2. shall require proof of access from the maintenance staff working on the electronic information system;

3.2.1.19.1.3. shall give authorization to the persons belonging to the body with the required access rights and technical expertise to supervise the maintenance activities of persons without the required privileges.

3.2.1.19.2. Maintenance with enhanced security measures

3.2.1.19.2.1. The body concerned:

3.2.1.19.2.1.1. when employing maintenance staff who do not have the appropriate safety clearance:

3.2.1.19.2.1.1.1. shall keep such maintenance staff under the supervision of technically qualified internal persons with appropriate access rights during the maintenance and diagnostic activities on electronic information systems,

3.2.1.19.2.1.1.2. before starting maintenance and diagnostic activities, shall delete all available information storage elements of electronic information systems and shall remove non-erasable data carriers or physically disconnect from the system;

3.2.1.19.2.1.2. shall develop alternative security protection, if an electronic information system element cannot be deleted, removed or disconnected from the system.

3.2.1.19.3. Timely repair

The body concerned shall obtain maintenance support to specified electronic information system elements.

3.3. LOGICAL SECURITY MEASURES

3.3.1. GENERAL SECURITY MEASURES

3.3.1.1. The body concerned:

3.3.1.1.1. shall develop and document according to the requirements applicable to the body concerned, and promulgate the authorization processes related to electronic information security (including system and user, external and internal access authorization) within the body concerned;

3.3.1.1.2. shall supervise the security status of the electronic information system and the environment;

3.3.1.1.3. shall determine roles and responsibilities related to information security, shall designate the persons to these positions;

3.3.1.1.4. shall integrate electronic information security authorization processes into the risk management process on the organizational level, in compliance with the information security policy and rules.

3.3.1.2. Electronic information security authorization shall cover all:

3.3.1.2.1. human, physical and logical resources;

3.3.1.2.2. procedural and protection levels and processes

falling within the competence of the organization concerned.

3.3.1.3. Connections of electronic information systems

3.3.1.3.1. The body concerned:

3.3.1.3.1.1. shall regulate and may impose an internal authorization process for the connections of electronic information systems to other electronic information systems;

3.3.1.3.1.2. shall document the given connections, interface parameters, security requirements and the type of electronic information transmitted over the connection.

3.3.1.3.2. Internal system connections

The body concerned shall impose an internal authorization process for the connections between its electronic information systems.

3.3.1.3.3. Restrictions on external connections

The body concerned shall set up and apply a set of rules on connections to external electronic information systems in the information security policy and rules which may result in enabling or disabling all connections, enabling or disabling specific connections.

3.3.1.4. Safety of persons

3.3.1.4.1. All personal safety procedures or expectations shall cover the entire staff of the body concerned and all natural persons who get or may get in contact with the electronic information systems of the body concerned. In cases where the person coming in actual or presumed contact with its electronic information systems is not the member of the body concerned, the above shall be enforced during the conclusion of the contract, agreement establishing the legal relationship forming the base of the activity as an obligation (including but not limited to commitments to getting to know and abiding by the regulations, the rules of procedure as well as the confidentiality declaration).

3.3.2. PLANNING

3.3.2.1. Security planning policy

3.3.2.1.1. The body concerned:

3.3.2.1.1.1. shall develop and document according to the requirements applicable to the body concerned, and promulgate the security planning policy to the persons concerned based on their positions and job descriptions which contains security planning processes and shall ensure its monitoring;

3.3.2.1.1.2. shall review and update the security planning policy with a frequency specified in the security planning policy or in other internal regulations.

3.3.2.2. System security plan

3.3.2.2.1. The body concerned, if the planning of electronic information systems belongs to its competence, shall develop the system security plan to the electronic information system, which:

3.3.2.2.1.1. is consistent with its organizational structure or its organizational-level architecture;

3.3.2.2.1.2. determines the scope of the electronic information system, its core tasks (its services to be provided), its security-critical elements and core functions;

3.3.2.2.1.3. determines the security classes under laws of the electronic information system and the data processed by it;

3.3.2.2.1.4. determines the operating conditions of the electronic information system and its connections with other electronic information systems;

3.3.2.2.1.5. incorporates security requirements of electronic information systems in the relevant system documentation;

3.3.2.2.1.6. determines recent or planned security measures meeting the requirements and measure expansions, performs statutory security duties;

3.3.2.2.1.7. ensures that persons working in specific positions and roles shall get to know the system security plan (including its changes, too);

3.3.2.2.1.8. reviews the system security plan of electronic information systems with a frequency specified in internal regulations or in the system security plan;

3.3.2.2.1.9. updates the system security plan in case of changes in the electronic information system or its operating environment, and problems identified during the implementation of the plan or the assessment of security measures;

3.3.2.2.1.10. carries out the necessary internal consultations;

3.3.2.2.1.11. ensures that the system security plan cannot be learnt or modified by unauthorized persons.

3.3.2.3. Action plan

3.3.2.3.1. The body concerned:

3.3.2.3.1.1. shall prepare an action plan, if deficiencies are identified at the security classification regarding the given electronic information system;

3.3.2.3.1.2. shall document - in the action plan - the planned activities to rectify deficiencies identified and to reduce or eliminate the known vulnerabilities of electronic information systems;

3.3.2.3.1.3. shall update the existing action plan with a frequency specified by the body concerned, based on the results of security assessments, security impact assessments and continuous surveillance.

3.3.2.4. Personal security

3.3.2.4.1. The body concerned:

3.3.2.4.1.1. shall develop and document according to the requirements applicable to the body concerned, and promulgate the expectations towards the persons, users requesting access rights to electronic information systems, the rules applicable to them, their responsibilities and the mandatory or prohibited activity related to the given system;

3.3.2.4.1.2. shall require a written statement from the persons, users requesting access rights before access authorization to electronic information systems, who certify with their statements that they have learnt the security rules and obligations related to the use of the electronic information systems and applicable to them, and abide by them at their own risk;

3.3.2.4.1.3. shall review and update the expectations towards the persons, users requesting access rights to electronic information systems, the rules applicable to them, their responsibilities and the mandatory or prohibited activity related to the given system, compliance with the code of conduct;

3.3.2.4.1.4. shall ensure that in case of change under point 3.3.2.4.1.3 the procedure defined in point 3.3.2.4.1.2 is carried out regarding the persons having access;

3.3.2.4.1.5. shall determine the requirements directed outside the body concerned.

3.3.2.5. Information security architecture description

3.3.2.5.1. The body concerned (if it falls within its scope and if it is not specified in other documents, or does not follow from them):

3.3.2.5.1.1. shall prepare the information security architecture description of the electronic information systems;

3.3.2.5.1.2. shall review and update the information security architecture description, in response to changes in its overall architecture;

3.3.2.5.1.3. shall ensure that the change planned in the information security architecture description reflects in the system security plan and in procurements.

3.3.2.5.2. Information security architecture description:

3.3.2.5.2.1. shall summarize the philosophy, requirements and approach to the protection of secrecy, integrity and availability of the electronic information system;

3.3.2.5.2.2. shall determine how the information security architecture fits into the overall architecture of the body and how it supports the overall infrastructure;

3.3.2.5.2.3. shall describe information security assumptions and dependencies regarding external services.

3.3.3. SYSTEM AND SERVICE PROCUREMENT

3.3.3.1. The procedures determined in this title shall not be introduced at the body concerned, if it does not procure IT services or devices in its own competence, and does not carry out or make system development activity carried out (excluding the typically low-value, commercially available, usually office applications, software or those hardware procurements which aim the replacement of damaged devices or expanding the equipment with the same or similar devices, as well as the procurement for repair, maintenance). For the purposes of this chapter, procurement and update of commercially available software does not constitute development.

3.3.3.2. Development lifecycle of systems

3.3.3.2.1. The body concerned:

3.3.3.2.1.1. shall monitor the IT security situation of its electronic information systems throughout their course of life, in all their lifecycles;

3.3.3.2.1.2. shall determine and document information security roles and responsibilities throughout the whole development lifecycle;

3.3.3.2.1.3. shall determine and designate responsible persons having information security roles according to the rules applicable to the body.

3.3.3.2.2. The stages of the system lifecycle are the followings:

3.3.3.2.2.1. requirement definition;

3.3.3.2.2.2. development or procurement;

3.3.3.2.2.3. implementation or assessment;

3.3.3.2.2.4. operation and maintenance;

3.3.3.2.2.5. extraction (archiving, destruction).

3.3.3.3. Functions, ports, protocols, services

The body concerned requires that the service provider determines the functions, protocols, ports and other services necessary to use the services.

3.3.3.4. Developer change tracking

3.3.3.4.1. The body concerned requires the followings from the developer of the electronic information system, system element or system service:

3.3.3.4.1.1. it shall implement the changes during planning, developing, implementing, operating of the electronic information system, system element or system service;

3.3.3.4.1.2. it shall document, handle and control the changes, shall ensure their integrity;

3.3.3.4.1.3. it shall carry out only the approved changes on the electronic information system, system element or system service;

3.3.3.4.1.4. it shall document the approved changes and their possible security impacts;

3.3.3.4.1.5. it shall monitor security defects and their corrections of the electronic information system, system element or system service, and shall notify its remarks to the persons determined by the body concerned.

3.3.3.5. Developer security testing

3.3.3.5.1. The body concerned requires the followings from the developer of the electronic information system, system element or system service:

3.3.3.5.1.1. it shall prepare a security assessment plan, and implement the rules contained therein;

3.3.3.5.1.2. it shall carry out unit, integration, system, or regression testing (in a way that fits the development), and assess it with a coverage and depth specified by the body concerned;

3.3.3.5.1.3. it shall document that the rules in the security assessment plan are implemented, and shall present the results of security testing and assessment;

3.3.3.5.1.4. it shall rectify deficiencies identified during security testing and assessment.

3.3.3.6. Development process, standards and devices

3.3.3.6.1. The body concerned:

3.3.3.6.1.1. requires from the developer of the electronic information system, system element or system service to follow documented development processes;

3.3.3.6.1.2. prescribes that the developer shall review the development processes, standards, devices and device options, configurations with a frequency specified by the body concerned for the compliance with the security requirements laid down by it.

3.3.3.6.2. The documented development process:

3.3.3.6.2.1. shall handle security requirements with high priority;

3.3.3.6.2.2. shall determine standards and devices used in development;

3.3.3.6.2.3. shall document special device options and configurations used during development;

3.3.3.6.2.4. shall keep a record about changes, and shall ensure the protection against their unauthorized modification.

3.3.3.7. Developer education

The body concerned shall impose an educational obligation on the developer of the electronic information system, system element or system service so that the persons designated by the body concerned (especially administrators) and security officers can familiarize themselves with and learn the correct use and operation of the security functions, measures and mechanisms implemented.

3.3.3.8. Developer security architecture and design

3.3.3.8.1. The body concerned requires the establishment of such specification and security architecture from the developer of the electronic information system, system element or system service which:

3.3.3.8.1.1. fits into and supports the security architecture of the organization;

3.3.3.8.1.2. describes the required security functions and the separation of security measures among physical and logical components;

3.3.3.8.1.3. presents the interoperability of each security function, mechanism and service in the implementation of the required security requirements as well as in a uniform approach to protection.

3.3.4. SECURITY ANALYSIS

3.3.4.1. Security analysis rules of procedure

3.3.4.1.1. The body concerned:

3.3.4.1.1.1. shall develop and document according to the requirements applicable to the body concerned, and promulgate the rules of security assessment procedures within the body concerned which facilitates the implementation of the security assessment policy and the related control;

3.3.4.1.1.2. shall review and update the security assessment procedures with a frequency specified in the rules of security assessment procedures or in other internal regulations.

3.3.4.2. Security assessments

3.3.4.2.1. The body concerned:

3.3.4.2.1.1. shall prepare a security assessment plan;

3.3.4.2.1.2. shall assess the security measures of the electronic information systems and the operating environment with a specified frequency, and shall control the functioning of the measures introduced and the operation as planned;

3.3.4.2.1.3. shall prepare a report summarizing the results of the security assessment;

3.3.4.2.1.4. shall ensure that the report summarizing the results of the security assessment shall be learnt by the persons holding specific roles determined by the body concerned or in accordance with the privileges of the role.

3.3.4.2.2. The security assessment shall contain:

3.3.4.2.2.1. the (administrative, physical and logical) security measures to be assessed;

3.3.4.2.2.2. the rules of procedure for determining the effectiveness of security controls;

3.3.4.2.2.3. the assessment environment, the assessment team, the purpose of the assessment, the task of the evaluators.

3.3.4.3. Special assessments

The body concerned shall make vulnerability testing, malicious user testing, internal threat assessment, source code analysis of security-critical custom-developed software components, other security assessments specified by the body concerned in the context of the assessment of security measures, with or without notification.

3.3.4.4. Measuring security performance

The body concerned shall develop and supervise the security measurement system of electronic information systems.

3.3.5. TESTING, TRAINING AND SUPERVISION

3.3.5.1. The body concerned:

3.3.5.1.1. if it falls within its scope, shall develop and document according to the requirements applicable to the body concerned, and promulgate the procedures related to testing, training and supervision of electronic information systems which support:

3.3.5.1.1.1. the development and maintenance of testing, training and supervision activities;

3.3.5.1.1.2. the continuous timely implementation of testing, training and supervision activities;

3.3.5.1.1.3. to review testing, training and supervision plans based on the risk management strategy and the severity of potential or actual security incidents.

3.3.5.2. Measuring security performance

The body concerned shall develop and supervise the security measurement system of its electronic information systems.

3.3.5.3. Vulnerability test

3.3.5.3.1. The body concerned:

3.3.5.3.1.1. shall perform vulnerability testing regarding its electronic information systems and their applications, if the electronic information system development, operation and use conditions make it possible;

3.3.5.3.1.2. shall repeat vulnerability testing with a specified frequency or at random or in the event that a new potential vulnerability arises in relation to the electronic information system or its application;

3.3.5.3.1.3. shall perform vulnerability testing using vulnerability testing devices and techniques or involving an external body regarding the electronic information systems which are under the supervision and control of the body concerned;

3.3.5.3.1.4. shall prepare a statement of the errors detected and incorrect configuration settings;

3.3.5.3.1.5. shall implement checklists and testing procedures;

3.3.5.3.1.6. shall assess the potential impacts of the vulnerability;

3.3.5.3.1.7. shall analyse the result of the vulnerability test;

3.3.5.3.1.8. shall share the result of the vulnerability test with the persons and roles determined by the body concerned.

3.3.5.3.2. Update capability

The body concerned shall use a vulnerability test device the vulnerability detection capability of which can be easily expanded as vulnerabilities become known.

3.3.5.3.3. Update from time to time, before a new examination or after detection of a new vulnerability

The body concerned shall update the scope of the vulnerability examined for the electronic information system before the new test or immediately after the vulnerability is discovered.

3.3.5.3.4. Privileged access

The electronic information system shall ensure access being subject to special permission (so-called privileged access) to the system elements designated by the body concerned for the purpose of performing the vulnerability test.

3.3.5.3.5. Disclosable information

The body concerned shall determine what kind of information an attacker may access in the electronic information system, and shall make repairs to prevent it.

3.3.6. CONFIGURATION MANAGEMENT

3.3.6.1. Configuration management rules of procedures

3.3.6.1.1. The body concerned:

3.3.6.1.1.1. shall develop and document according to the requirements applicable to the body concerned, and promulgate the rules of configuration management procedures within the body concerned which facilitates the implementation of configuration management policy and the controls related thereto;

3.3.6.1.1.2. shall review and update the rules of configuration management procedures with a frequency specified in the rules of physical security procedures or in other internal regulations.

3.3.6.2. Basic configuration

3.3.6.2.1. The body concerned shall develop a basic configuration for each electronic information system, shall document and maintain as well as include the essential elements of the system in an inventory.

3.3.6.2.2. Reviews and updates

The basic configurations shall be updated as an integral part of installation and updating of electronic information system elements.

3.3.6.2.3. Preservation of previous configurations

The basic configuration and its further versions of the electronic information system shall be kept unchanged in order that, if necessary, the return thereto may be possible.

3.3.6.2.4. Configuration of high-risk areas

3.3.6.2.4.1. Electronic information system elements or devices configurated in a manner determined for security reasons shall be provided to the persons who use the electronic information system at an external site.

3.3.6.2.4.2. Appropriate security procedures shall be applied when the device under point 3.3.6.2.4.1 is put into internal use.

3.3.6.2.5. Automatic support

Automatic mechanisms shall be applied to maintain an up-to-date, complete, accurate and permanently available basic configuration of the electronic information system.

3.3.6.3. Oversight of configuration changes (change management)

3.3.6.3.1. The body concerned:

3.3.6.3.1.1. shall define the types of changes that are subject to change management oversight;

3.3.6.3.1.2. shall define the mandatory and non-mandatory elements and preconditions of the change management oversight in case of certain types of changes (attached documentation, test reports, etc.);

3.3.6.3.1.3. shall examine the proposed changes submitted to change management oversight, then shall approve or reject them based on risk analysis;

3.3.6.3.1.4. shall document the decisions regarding the changes in electronic information systems;

3.3.6.3.1.5. shall implement the approved changes in electronic information systems;

3.3.6.3.1.6. shall retrievably preserve the documents of changes in the electronic information system, and their detailed description;

3.3.6.3.1.7. shall audit and review activities related to changes under configuration change oversight.

3.3.6.3.2. Preliminary testing and confirmation

Before changing the configuration, the new version shall be tested, then a decision on its adequacy shall be made, and the changes in electronic information systems shall be documented before being implemented in a live system.

3.3.6.3.3. Automatic support

3.3.6.3.3.1. Automatic mechanisms shall be applied to:

3.3.6.3.3.1.1. document proposed changes in electronic information systems;

3.3.6.3.3.1.2. notify the persons entitled to approve;

3.3.6.3.3.1.3. highlight late approvals;

3.3.6.3.3.1.4. prevent the implementation of changes not yet approved;

3.3.6.3.3.1.5. fully document changes implemented in electronic information systems;

3.3.6.3.3.1.6. notify the persons entitled to approve about the implementation of approved changes.

3.3.6.4. Security impact assessment

3.3.6.4.1. The body concerned shall examine the impact of the changes planned in electronic information systems on information security, even before the changes are implemented.

3.3.6.4.2. Isolated test environment

The body concerned shall examine the changes in an isolated test environment before they are implemented in a live system, looking for bugs, vulnerabilities, compatibility issues and signs of intentional damage.

3.3.6.5. Access restrictions regarding changes

3.3.6.5.1. The body concerned shall determine access rights to changes in its regulation regarding the electronic information system, shall document the access rights and approve them, shall apply physical and logical access restrictions in relation to the changes in the electronic information system.

3.3.6.5.2. Automatic support

The body concerned shall apply automatic mechanisms in the electronic information system for access restrictions, to log activities related thereto.

3.3.6.5.3. Review

The body concerned shall regularly review the changes of the electronic information system to determine whether an unauthorized change has been made.

3.3.6.5.4. Signed elements

In case of software and so-called firmware elements (control devices) determined by the body, the installation of elements shall be prevented, if they are not digitally signed, using a known and approved certificate.

3.3.6.6. Configuration settings

3.3.6.6.1. The body concerned:

3.3.6.6.1.1. shall determine the configuration settings mandatory for information technology products used in electronic information systems in a way that they still meet operational requirements, but are as limited as possible from a security point of view based on 'necessary minimum' principle, and shall document it as a checklist;

3.3.6.6.1.2. shall perform configuration settings in all elements of electronic information systems;

3.3.6.6.1.3. shall identify, document and approve every derogation in the configuration settings of specified elements;

3.3.6.6.1.4. shall monitor and control the changes in configuration settings in compliance with the internal regulations and procedures of the body concerned.

3.3.6.6.2. Automatic support

The body concerned shall apply automatic mechanisms regarding the electronic information system to centrally manage, apply and control configuration settings.

3.3.6.6.3. Reaction to unauthorized changes

The body concerned shall introduce specified measures in case of unauthorized changes in determined configuration settings.

3.3.6.7. Narrowest functionality

3.3.6.7.1. The body concerned:

3.3.6.7.1.1. shall configure the electronic information system to provide the necessary services only;

3.3.6.7.1.2. shall determine the use of prohibited or restricted, unnecessary functions, ports, protocols, services, software.

3.3.6.7.2. Regular review

3.3.6.7.2.1. The body concerned shall review the electronic information systems with a specified frequency, shall determine and block or disable unnecessary or unsafe functions, ports, protocols, services, software.

3.3.6.7.2.2. In compliance with the regulations for software use of the body concerned and its terms and conditions of software use, the electronic information system shall prevent running prohibited programs.

3.3.6.7.3. Non-executable software

The body concerned shall determine, regularly review and update the list of non-executable (banned, so-called blacklisted) software programs in the electronic information system and shall prohibit them from running.

3.3.6.7.4. Executable software

The body concerned shall determine, regularly review and update the list of executable (permitted, so-called whitelisted) software programs in the electronic information system and shall permit their running, and shall make the running of other software programs subject to individual permission.

3.3.6.8. Electronic information system element inventory

3.3.6.8.1. The body concerned:

3.3.6.8.1.1. shall make an inventory about electronic information system elements;

3.3.6.8.1.2. shall review and update the electronic information system element inventory with a specified frequency;

3.3.6.8.1.3. shall ensure that the inventory:

3.3.6.8.1.3.1. accurately reflects the current status of electronic information systems;

3.3.6.8.1.3.2. contains all hardware and software components falling within the scope of electronic information systems;

3.3.6.8.1.3.3. shall be sufficiently detailed for tracking and reporting.

3.3.6.8.2. Update

The body concerned shall update the electronic information system element inventory at the time of installation, removal or update of certain system elements.

3.3.6.8.3. Automatic detection of unauthorized items

3.3.6.8.3.1. Automated mechanisms ensure that unauthorized hardware, software and firmware items shall be detected with a frequency specified by the body concerned.

3.3.6.8.3.2. In case of detection of unauthorized items, network access by such items shall be disabled, they shall be isolated and the competent persons shall be notified.

3.3.6.8.4. Protection against duplication

The body concerned shall control whether the items within the scope of the electronic information system are included in an inventory of other electronic information systems.

3.3.6.8.5. Automatic support

The body concerned shall apply automatic mechanisms regarding the electronic information system to support the up-to-date, complete, accurate and constantly available management of electronic information system element inventory.

3.3.6.8.6. Logging

The name, position and role of the persons responsible for administration of the items concerned shall be attached to the electronic information system element inventory.

3.3.6.9. Configuration management plan

3.3.6.9.1. The body concerned:

3.3.6.9.1.1. shall develop, document and implement a configuration management plan regarding electronic information systems which shall take the roles, responsibilities, configuration management processes and processes into consideration;

3.3.6.9.1.2. shall introduce a process for identification of configuration elements during the system development lifecycle and for configuration management of configuration elements;

3.3.6.9.1.3. shall determine the configuration elements of electronic information systems., and shall place configuration elements under configuration management;

3.3.6.9.1.4. shall protect the configuration management plan against unauthorized disclosure and modification.

3.3.6.10. Restrictions on use of software

3.3.6.10.1. The body concerned:

3.3.6.10.1.1. shall only use software programs and related documentation that meet the contractual requirements applicable to them and the copyright or other laws;

3.3.6.10.1.2. shall monitor the use of volume licensed software and related documentation to check copies, sharing;

3.3.6.10.1.3. shall control and document file sharing to ascertain that this opportunity is not used for unauthorized sharing, publishing, implementing or reproducing of copyrighted work.

3.3.6.11. User-installed software

3.3.6.11.1. The body concerned:

3.3.6.11.1.1. shall develop regarding the electronic information system, shall document according to the requirements applicable to the body and promulgate the rules within the body which determine the opportunity for users to install software;

3.3.6.11.1.2. shall enforce the rules of software installation according to the methods specified by the body concerned;

3.3.6.11.1.3. shall control the compliance with the rules with a specified frequency.

3.3.7. MAINTENANCE

3.3.7.1. System maintenance rules of procedure

3.3.7.1.1. The body concerned:

3.3.7.1.1.1. shall develop and document according to the requirements applicable to the body concerned, and promulgate the rules of system maintenance procedures within the body concerned, which facilitates the implementation of system maintenance management policy and the controls related thereto;

3.3.7.1.1.2. shall review and update the rules of system maintenance procedures with a frequency specified in the rules of physical security procedures or in other internal regulations.

3.3.7.2. Regular maintenance

3.3.7.2.1. The body concerned:

3.3.7.2.1.1. shall perform maintenance and repairs on a scheduled basis, shall document and review the records of maintenance and repairs in compliance with the manufacturer's or distributor's specifications and organizational requirements;

3.3.7.2.1.2. shall approve and control all maintenance activities, regardless of whether they are performed on-site or remotely, and regardless of whether the equipment is maintained on site or elsewhere;

3.3.7.2.1.3. shall require the approval of the persons responsible therefor to deliver electronic information systems or system elements from the facilities of the body;

3.3.7.2.1.4. shall delete - after saving - all data and information from the equipment before delivery;

3.3.7.2.1.5. shall check whether the equipment continues to function properly also after maintenance or repair activities and shall subject it to security screening;

3.3.7.2.1.6. shall attach the determined information related to maintenance to the maintenance records.

3.3.7.2.2. Automatic support

3.3.7.2.2.1. The body concerned:

3.3.7.2.2.1.1. shall apply automated mechanisms to schedule, carry out and document maintenance and repairs;

3.3.7.2.2.1.2. shall make an up-to-date, accurate and complete record about all required, scheduled, ongoing and completed maintenance and repair actions.

3.3.7.3. Maintenance tools

3.3.7.3.1. Regarding the electronic information system, the body concerned shall approve, record and check the maintenance tools of the electronic information system.

3.3.7.3.2. Data carrier control

The body concerned shall check data carriers containing diagnostic and test programs regarding malicious codes, before they are used in the electronic information system.

3.3.7.4. Remote maintenance

3.3.7.4.1. The body concerned:

3.3.7.4.1.1. shall approve, monitor and control remote maintenance and diagnostic activities;

3.3.7.4.1.2. allows the use of remote maintenance and diagnostic devices, if it is in compliance with information security policy and rules and is documented in the system security plan of the electronic information system;

3.3.7.4.1.3. shall use authentications when creating remote maintenance and diagnostic work phases;

3.3.7.4.1.4. shall keep a record of remote maintenance and diagnostic activities;

3.3.7.4.1.5. shall close the work phase and network connections when remote maintenance is complete.

3.3.7.4.2. Documentation

The body concerned shall document the rules and procedures for establishing and using remote maintenance and diagnostic connections in the system security plan of the electronic information system.

3.3.7.4.3. Comparable security

3.3.7.4.3.1. The body concerned requires that remote maintenance and diagnostic repairs shall be carried out from an electronic information system in which security capabilities are at the same level as the serviced system security capabilities.

3.3.7.4.3.2. If the procedure under point 3.3.7.4.3.1 is not ensured, the element to be serviced shall be removed from the electronic information system, and before remote maintenance and diagnostic repairs, all information shall be deleted from the system element concerned.

3.3.7.4.3.3. If the procedure under points 3.3.7.4.3.1 or 3.3.7.4.3.2 cannot be carried out, after performing service, the element shall be examined for possible malware before reconnecting it to the electronic information system.

3.3.8. DATA CARRIER PROTECTION

3.3.8.1. Data carrier protection rules of procedure

3.3.8.1.1. The body concerned:

3.3.8.1.1.1. shall develop and document according to the requirements applicable to the body concerned, and promulgate the rules of data carrier protection procedures within the body concerned, which facilitates the implementation of data carrier protection policy and the controls related thereto;

3.3.8.1.1.2. shall review and update the rules of data carrier protection procedures with a frequency specified in the rules of data carrier protection procedures or in other internal regulations.

3.3.8.2. Access to data carriers

The body concerned shall determine the circle of persons entitled to access to specified data carrier types and the content of their license.

3.3.8.3. Labelling of data carriers

The body concerned shall label data carriers of the electronic information system, indicating restrictions on the dissemination of information, warnings for handling and safety signs, if available.

3.3.8.4. Storage of data carriers

3.3.8.4.1. The body concerned:

3.3.8.4.1.1. shall physically check and securely store data carriers in an authorized or designated place;

3.3.8.4.1.2. shall protect data carriers of the electronic information system so long as data carriers are destroyed or deleted by approved means, techniques and procedures.

3.3.8.5. Transport of data carriers

3.3.8.5.1. The body concerned:

3.3.8.5.1.1. shall protect and control data carriers of the electronic information system with specific security precautions during transport outside controlled areas;

3.3.8.5.1.2. shall ensure accountability of data carriers during transport outside controlled areas;

3.3.8.5.1.3. shall document activities related to transportation of data carriers;

3.3.8.5.1.4. shall restrict activities related to transportation of data carriers to the person entitled thereto.

3.3.8.5.2. Cryptographic protection

Cryptographic mechanisms shall be applied to protect confidentiality and integrity of the information stored on digital data carriers during transportation outside controlled areas.

3.3.8.6. Deletion of data carriers

3.3.8.6.1. The body concerned:

3.3.8.6.1.1. shall delete the determined data carriers of the electronic information system with erasure techniques and procedures ensuring irreversibility before scrapping, cessation of organizational control or release for re-use;

3.3.8.6.1.2. shall apply erasure mechanisms according to the strength and integrity in concert with the rating category of the information.

3.3.8.6.2. Control

The body concerned shall review, approve, monitor, document and control the activities related to erasure and destruction of data carriers.

3.3.8.6.3. Testing

Devices and procedures applied to deletion shall be tested with a specified frequency.

3.3.8.6.4. Deletion without destruction

Non-destructive deletion techniques shall be applied to specified portable storage devices, before such devices are connected to the electronic information system.

3.3.8.7. Using data carriers

3.3.8.7.1. The body concerned shall permit, restrict or forbid the use of certain or any data carrier types by using security measures operating in determined electronic information systems or system elements.

3.3.8.7.2. Unknown owner

The body concerned shall forbid the use of portable data carriers in electronic information systems owner of which cannot be identified.

3.3.9. IDENTIFICATION AND AUTHENTICATION

3.3.9.1. Identification and authentication rules of procedures

3.3.9.1.1. The body concerned:

3.3.9.1.1.1. shall develop and document according to the requirements applicable to the body concerned, and promulgate the rules of identification and authentication procedures within the body concerned, which facilitates the implementation of identification and authentication policy and the controls related thereto;

3.3.9.1.1.2. shall review and update the rules of identification and authentication procedures with a frequency specified in the rules of identification and authentication procedures or in other internal regulations.

3.3.9.2. Identification and authentication

3.3.9.2.1. The electronic information system shall individually identify and authenticate the bodies' users and the activities carried out by the users.

3.3.9.2.2. Network access to privileged accounts

The electronic information system shall use multi-factor authentication to the network access to user accounts with special privileges (so-called privileged accounts).

3.3.9.2.3. Network access to non-privileged accounts

The electronic information system shall use multi-factor authentication to the network access to non-privileged accounts.

3.3.9.2.4. Local access to privileged accounts

The electronic information system shall use multi-factor authentication to the local access to privileged accounts.

3.3.9.2.5. Replay protection

The electronic information system shall use authentication mechanisms ensuring replay protection to the network access to privileged accounts.

3.3.9.2.6. Remote access - separate device

The electronic information system shall use multi-factor authentication to the remote access to user accounts, and one of the factors preceding access is a device separated from the electronic information system which meets the defined security requirements.

3.3.9.2.7. Local access to non-privileged accounts

The electronic information system shall use multi-factor authentication to the local access to non-privileged accounts.

3.3.9.2.8. Replay-protected network access to non-privileged accounts

The electronic information system shall use authentication mechanisms ensuring replay protection to the network access to non-privileged accounts.

3.3.9.3. Device identification and authentication

The electronic information system shall individually identify and authenticate the specified devices and device types before establishing a local or remote network connection with them.

3.3.9.4. Identities management

3.3.9.4.1. The body concerned:

3.3.9.4.1.1. shall stipulate the assignment of individual, group, role or device identifiers to the permission of persons or roles determined by the body;

3.3.9.4.1.2. shall assign the identifier to the desired individual, group, role or device;

3.3.9.4.1.3. shall prevent the repeated use of identifiers for a specified period;

3.3.9.4.1.4. shall disable the identifier in the event of a specified period of inactivity.

3.3.9.5. Management of authentication devices

3.3.9.5.1. The body concerned:

3.3.9.5.1.1. shall control the permission of the persons, groups, roles receiving the device or that of the devices when allocating authentication devices;

3.3.9.5.1.2. shall specify the initial content of the authentication devices;

3.3.9.5.1.3. shall ensure the permissions corresponding the intended use of the authentication device;

3.3.9.5.1.4. shall document the allocation, revocation and exchange of authentication devices, lost or compromised or damaged devices;

3.3.9.5.1.5. shall change the default value of authentication devices during the installation of electronic information systems;

3.3.9.5.1.6. shall specify the minimum and maximum service life of authentication devices and the conditions for re-use;

3.3.9.5.1.7. shall change or update authentication devices at intervals specified for the types of authentication devices;

3.3.9.5.1.8. shall protect the content of authentication devices against unauthorized disclosure and modification;

3.3.9.5.1.9. shall require from the users of authentication devices to protect the secrecy and integrity of their devices;

3.3.9.5.1.10. shall replace the authentication device when changing accounts concerned.

3.3.9.5.2. Password-based (knowledge-based) authentication

3.3.9.5.2.1. The body concerned:

3.3.9.5.2.1.1. shall apply the following requirements to the password: case sensitive; determining the number of characters; lowercase, uppercase, numbers and special characters and minimum password length;

3.3.9.5.2.1.2. shall force a specified number of character changes when setting a new password;

3.3.9.5.2.1.3. shall not store passwords (excluding storing the split value generated from the password with the irreversible cryptographic splitting function), and shall not forward them;

3.3.9.5.2.1.4. shall impose a minimum and a maximum lifetime limit on passwords in the way that prohibits the reuse of passwords up to a specified number of new passwords, requires to change the temporary password allowing the first access into the system.

3.3.9.5.3. Possession-based authentication

3.3.9.5.3.1. The body concerned:

3.3.9.5.3.1.1. shall use a mechanism for hardware token-based authentication of electronic information systems which meets the quality requirements set by the body concerned, or

3.3.9.5.3.1.2. for public key infrastructure-based authentication of electronic information systems:

3.3.9.5.3.1.2.1. shall control certificates by building and verifying a certificate chain up to an accepted trusted point, including certificate status information check, too;

3.3.9.5.3.1.2.2. shall force authorized access to the corresponding private key;

3.3.9.5.3.1.2.3. shall associate the authenticated identity with the individual or group account;

3.3.9.5.3.1.2.4. shall implement local storage of revocation data for the support of the build-up and verification of the certificate chain in case where revocation data are not available via networks.

3.3.9.5.4. Inherence-based authentication

The body concerned shall carry out authentication based on the users' characteristics allowing unique identification.

3.3.9.5.5. Registration personally or by a reliable third party

The body concerned shall require a registration procedure to receive a specific authentication device which is carried out by a specified registration body with the approval of the persons or roles determined by the body concerned.

3.3.9.6. Feedback of the authentication device

The electronic information system shall provide covered feedback during the authentication process in order to protect authentication information from the possible disclosure and use by unauthorized persons.

3.3.9.7. Authentication for cryptographic module

The electronic information system shall use a mechanism to authentication for a given cryptographic module which is in compliance with the cryptographic module authentication guide.

3.3.9.8. Identification and authentication (users outside the body)

3.3.9.8.1. The electronic information system shall individually identify and authenticate the users outside the body concerned and their activities.

3.3.9.8.2. Accepting certificates of authentication service providers

The electronic information system shall only accept the certificates issued by the certification-service-providers included in the electronic signature register of the National Media and Communications Authority (NMHH) to authenticate users outside the body concerned.

3.3.10. ACCESS CHECK

3.3.10.1. Access check rules of procedures

3.3.10.1.1. The body concerned:

3.3.10.1.1.1. shall develop and document according to the requirements applicable to the body concerned, and promulgate the rules of access check procedures within the body concerned, which facilitates the implementation of the access check policy and the checks related thereto;

3.3.10.1.1.2. shall review and update the rules of procedure protecting access with a frequency specified in the rules of procedure protecting access or in other internal regulations.

3.3.10.2. Managing user accounts

3.3.10.2.1. The body concerned:

3.3.10.2.1.1. shall determine and identify user accounts of electronic information systems and their types;

3.3.10.2.1.2. shall designate account managers for user accounts;

3.3.10.2.1.3. shall establish group and role membership conditions;

3.3.10.2.1.4. shall specify the authorized users of electronic information systems, the group and role membership as well as the access permissions and, if necessary, additional features for each user account;

3.3.10.2.1.5. shall create, enable, modify, disable and remove user accounts in accordance with specified procedures or conditions;
3.3.10.2.1.6. shall monitor the use of user accounts;
3.3.10.2.1.7. shall notify account managers, if:
3.3.10.2.1.7.1. user accounts are no longer required,
3.3.10.2.1.7.2. users have quitted or reassigned,
3.3.10.2.1.7.3. use of the electronic information system or the knowledge necessary thereto has changed;
3.3.10.2.1.8. shall authorize access to electronic information systems based on:
3.3.10.2.1.8.1. valid access permission,
3.3.10.2.1.8.2. planned system use,
3.3.10.2.1.8.3. core tasks and functions;
3.3.10.2.1.9. shall review the user accounts and the compliance with account management requirements with a specified frequency;
3.3.10.2.1.10. shall establish a procedure for reissuing authentication devices or data associated with shared or group user accounts (if applied), in case of change in group members.
3.3.10.2.2. Automatic management
The electronic information system shall apply automated mechanisms to manage accounts of electronic information systems.
3.3.10.2.3. Removing temporary accounts
After a certain period of time has elapsed, the electronic information system shall automatically remove or disable temporary or emergency user accounts or certain designated user account types.
3.3.10.2.4. Disabling inactive accounts
The electronic information system shall automatically disable inactive accounts after a certain period of time has elapsed.
3.3.10.2.5. Automatic logging
The electronic information system shall automatically log the activities related to creating, modifying, permitting, disabling and removing accounts, and shall notify the persons and roles determined about it.
3.3.10.2.6. Logout
In case of expected inactivity of a specified duration or in other predetermined cases, the user shall be logged out.
3.3.10.2.7. Unusual use
The accounts of the electronic information system shall be monitored from the perspective of unusual use determined by the body concerned and shall report it to persons or roles determined.
3.3.10.2.8. Disabling
Accounts of users posing a risk shall be disabled immediately.
3.3.10.3. Enforcement of access check
The electronic information system shall enforce approved authorizations to logical access to information and to resources of the system in accordance with the relevant regulations.

3.3.10.4. Enforcement of information flow control

The electronic information system shall – in accordance with the relevant regulations - enforce approved authorization to control the information flow within and between related systems in accordance with the information flow control rules established by the body concerned.

3.3.10.5. Separation of responsibilities

3.3.10.5.1. The body concerned:

3.3.10.5.1.1. shall separate individual responsibilities;

3.3.10.5.1.2. shall document the separation of individual responsibilities;

3.3.10.5.1.3. shall determine the access permission to the electronic information system for the purpose of separating individual responsibilities.

3.3.10.6. Least privilege principle

3.3.10.6.1. The electronic information system shall apply the least privilege principle, namely it allows only the access necessary to perform the tasks assigned to the users or to the user activities.

3.3.10.6.2. Authorized access to security functions

The body concerned shall authorize access to specified security functions and security critical information.

3.3.10.6.3. Unprivileged access to security functions

The body concerned makes mandatory that the body's users with access to specified security functions and security critical information shall not use their accounts or role with special privileges (so-called privileged accounts or role) for the use of non-security functions.

3.3.10.6.4. Privileged accounts

The body concerned shall limit privileged accounts of electronic information systems to specified persons or roles.

3.3.10.6.5. Logging of the use of privileged functions

The electronic information systems shall log the implementation of privileged functions.

3.3.10.6.6. Blocking privileged functions for non-privileged users

The electronic information systems shall prevent non-privileged users from carrying out privileged functions, including disable, bypass or change security countermeasures.

3.3.10.6.7. Network access to privileged commands

Network access to determined privileged commands can only be authorized in a specific operational emergency and the justification of such access shall be documented in the system security plan. Privileged commands may only be issued from specific workstations, terminals, segments and IP addresses which workstation/terminal premises are assigned to a different level of classification from normal in terms of physical access.

3.3.10.7. Unsuccessful attempts to log-in

3.3.10.7.1. The electronic information system:

3.3.10.7.1.1. shall apply case number limit determined by the body concerned, for consecutive unsuccessful log-in attempts by the user within a specified period of time;

3.3.10.7.1.2. if the case number limit of unsuccessful log-in attempts is exceeded by the user, it shall automatically block the user account or hubs for a specified time period, or delay the next log-in attempt in a specified way.

3.3.10.8. System usage indication

3.3.10.8.1. By using electronic information systems, the body concerned:

3.3.10.8.1.1. shall send a warning message or signal for the system usage determined by the body concerned to users before allowing access to the system which indicates that:

3.3.10.8.1.1.1. the user uses the electronic information system of the body concerned;

3.3.10.8.1.1.2. the system usage may be monitored, recorded or logged;

3.3.10.8.1.1.3. the unauthorized use of the system is prohibited, and may result in criminal or civil liability;

3.3.10.8.1.1.4. the use of the system also means the user's consent to the above.

3.3.10.8.2. The electronic information system shall keep the warning message or signal on the screen until the user performs a direct operation to log in the electronic information system or to any further system access.

3.3.10.8.3. In case of publicly available systems, the electronic information systems:

3.3.10.8.3.1. shall display the conditions of use of the systems before granting further access;

3.3.10.8.3.2. if monitoring, data recording or logging takes place, shall display that these meet the data protection rules;

3.3.10.8.3.3. shall provide a description about the authorized use of the systems.

3.3.10.9. Simultaneous work phase management

The body concerned shall limit the number of simultaneous work phases to a number defined in the electronic information systems separately for specific accounts or account types.

3.3.10.10. Blocking of a work phase

3.3.10.10.1. The body concerned:

3.3.10.10.1.1. after a certain period of inactivity or in case of user action to that effect, shall prevent access to the electronic information system by blocking of the work phase;

3.3.10.10.1.2. shall keep the blocking of the work phase as long as the users identify and re-authenticate themselves by using appropriate procedures.

3.3.10.10.2. Screen capture

When blocking the work phase, the information previously displayed on the screen shall be captured with a publicly visible image (or with a blank screen) or with login interface which may contain also the name of the person blocking.

3.3.10.11. Closing the work phase

The electronic information system shall automatically close the work phase after conditions specified by the body concerned are met or after the occurrence of events requiring work phase disconnection.

3.3.10.12. Activities allowed without identification or authentication

3.3.10.12.1. The body concerned:

3.3.10.12.1.1. shall designate the user activities which may be carried out in the electronic information system without identification or authentication as well;

3.3.10.12.1.2. shall document and justify the user activities allowed without identification or authentication in the system security plan or in another regulation.

3.3.10.13. Remote access

3.3.10.13.1. The body concerned:

3.3.10.13.1.1. shall develop and document the restrictions of use for all allowed remote access types, configuration or connection requirements and implementation guidelines;

3.3.10.13.1.2. shall carry out an authorization process as a condition for remote access to the electronic information system.

3.3.10.13.2. Control

The electronic information system shall monitor and control remote accesses.

3.3.10.13.3. Encryption

Cryptographic mechanisms shall be applied for protecting secrecy and integrity of the work phases of remote access.

3.3.10.13.4. Access control points

Every remote access shall be managed through a supervised access control point in electronic information systems.

3.3.10.13.5. Access to privileged commands

3.3.10.13.5.1. The body concerned:

3.3.10.13.5.1.1. shall authorize remote access to execute privileged commands and to access to security critical information only in case of a defined and accepted demand;

3.3.10.13.5.1.2. shall document and justify the accesses in point 3.3.10.13.5.1.1 in the system security plan.

3.3.10.14. Wireless access

3.3.10.14.1. The body concerned:

3.3.10.14.1.1. shall issue restrictions on use, configuration and connection requirements as well as technical guidance regarding wireless technologies in internal regulations;

3.3.10.14.1.2. shall carry out an authorization process as a condition for wireless access.

3.3.10.14.2. Authentication and encryption

The body concerned shall protect wireless access in electronic information systems with encryption and by authenticating users or devices.

3.3.10.14.3. Disabling user configuration

The body shall identify the users and allow them the independent configuration of the wireless network only in possession of direct permission via wired connection over a secure network.

3.3.10.14.4. Antennas

The body concerned shall operate antennas and shielding solutions with characteristics and power levels or use another technique which reduce the probability of detecting signals outside the limits of physical protection of the body concerned.

3.3.10.15. Mobile device access control

3.3.10.15.1. The body concerned:

3.3.10.15.1.1. shall - in its internal regulations - issue restrictions on use, configuration and connection requirements as well as technical guidance regarding mobile devices it controls;

3.3.10.15.1.2. make connection with mobile devices to its electronic information systems subject to authorization.

3.3.10.15.2. Encryption

The body concerned shall use full device encryption, storage-based encryption or other technology to protect secrecy and integrity of the information stored on the mobile devices it determines or to make information inaccessible.

3.3.10.16. Use of external electronic information systems

3.3.10.16.1. The body concerned:

3.3.10.16.1.1. shall determine under what conditions and rules the user is entitled to access the electronic information systems from an external system;

3.3.10.16.1.2. shall determine how the user is authorized to process, store or transmit the information controlled by the body concerned by using external electronic information systems.

3.3.10.16.2. Restricted use

3.3.10.16.2.1. The body concerned shall permit the use of an external electronic information system to the authorized users to access the electronic information system, to process, store or transmit the information controlled by the body only in the case, if:

3.3.10.16.2.1.1. the existence of the necessary security measures on the external system is checked in advance in accordance with its own regulation, or

3.3.10.16.2.1.2. there is an approved connection between electronic information systems or an agreement is concluded with the body hosting the external electronic information system.

3.3.10.16.3. Portable storage devices

The body concerned shall restrict or forbid the use of controlled portable storage devices to the persons having access to external electronic information systems as well.

3.3.10.17. Information sharing

3.3.10.17.1. The body concerned:

3.3.10.17.1.1. shall facilitate information sharing that allows the authorized users to decide whether the permissions assigned to the sharing partner are in compliance with restrictions on access to information, in specific information sharing circumstances, when user judgment may be considered;

3.3.10.17.1.2. shall use automated mechanisms or manual processes to help users making information sharing or collaboration decisions.

3.3.10.18. Publicly available content

3.3.10.18.1. The body concerned:

3.3.10.18.1.1. shall designate the persons who are entitled to disclose any information related to the body concerned on publicly accessible electronic information systems;

3.3.10.18.1.2. shall provide training to the persons designated under point 3.3.10.18.1.1 to ensure that publicly accessible information does not include non-public information;

3.3.10.18.1.3. shall review the proposed content before publication;

3.3.10.18.1.4. shall review the publicly accessible content of the electronic information systems regarding non-public information with a specified frequency, and shall remove them.

3.3.11. SYSTEM AND INFORMATION INTEGRITY

3.3.11.1. These provisions shall be applied regarding a certain electronic information system, if the body concerned operates the given electronic information system. In case of operating service contract, the provisions in point 3.3.11. and its subpoints shall be enforced as a contractual obligation, and shall be provided by the service provider.

3.3.11.2. System and information integrity rules of procedure

3.3.11.2.1. The body concerned:

3.3.11.2.1.1. shall develop and document according to the requirements applicable to the body concerned, and promulgate the rules of system and information integrity procedures within the body concerned, which facilitates the implementation of system and information integrity policy, forming part of the information security policy and rules, and the controls related thereto;

3.3.11.2.1.2. shall review and update the rules of system and information integrity procedures with a frequency specified in the rules of system and information integrity procedures or in other internal regulations.

3.3.11.3. Error correction

3.3.11.3.1. The body concerned:

3.3.11.3.1.1. shall identify, report as per its internal rules of procedures and correct or make electronic information system errors corrected;

3.3.11.3.1.2. shall test software updates related to error correction before installation in terms of the effectiveness of task performance of the body concerned and the possible consequences;

3.3.11.3.1.3. shall install or make security critical software installed within a specified period after the release of their update;

3.3.11.3.1.4. shall incorporate error corrections into the configuration management process.

3.3.11.3.2. Automated error correction status

The body concerned shall apply automated mechanisms to determine the error correction status of its electronic information system elements.

3.3.11.3.3. Central management

The body concerned shall manage the error correction process centrally.

3.3.11.4. Malware protection

3.3.11.4.1. The body concerned:

3.3.11.4.1.1. shall protect its electronic information system at its entry and exit points against malware, shall detect and destroy them;

3.3.11.4.1.2. shall update protection mechanisms against malware in compliance with configuration management rules and procedures in all cases when updates appear for its anti-malware system;

3.3.11.4.1.3. shall configurate the malware protection mechanisms so that the means of protection:

3.3.11.4.1.3.1. shall carry out regular scans in the electronic information system, and perform real-time scanning of files from external sources at endpoints, at network entry or exit points in compliance with security policy, when files are downloaded, opened or executed,

3.3.11.4.1.3.2. if malware is detected, it shall block or quarantine it, and shall alert the system administrator and the further person(s) determined by the body concerned;

3.3.11.4.1.4. shall check for false alerts during detection and destruction of malware, and shall take their possible impact on the availability of the electronic information system into consideration.

3.3.11.4.2. Central management

The electronic information system shall manage the malware protection mechanisms centrally.

3.3.11.4.3. Automatic update

The electronic information system shall update the malware protection mechanisms automatically.

3.3.11.5. Supervision of electronic information systems

3.3.11.5.1. The body concerned:

3.3.11.5.1.1. shall supervise the electronic information system in order to detect cyberattacks or the signs of cyberattacks in accordance with the defined monitoring objectives, and to reveal unauthorized local, network and remote connections;

3.3.11.5.1.2. shall identify the unauthorized use of electronic information systems;

3.3.11.5.1.3. shall use supervisory tools to collect certain basic information and to follow up potentially important, special types of transactions in ad hoc areas of the system;

3.3.11.5.1.4. shall protect information obtained from intrusion monitoring devices against unauthorized access, modification and deletion;

3.3.11.5.1.5. shall strengthen the supervision of the electronic information system in all cases when an indication of increased risk is detected;

3.3.11.5.1.6. shall provide supervisory information on the electronic information system to determined persons and roles with a specified frequency.

3.3.11.5.2. Automation

Automated devices shall be applied to support near real-time investigation of incidents.

3.3.11.5.3. Supervision

The electronic information system shall monitor incoming and outgoing data traffic regarding unusual or unauthorized activities or circumstances.

3.3.11.5.4. Alerts

The electronic information system shall alert the competent persons and groups of the body concerned, when predetermined signs of threat or potential threat are detected.

3.3.11.6. Security alerts and information

3.3.11.6.1. The body concerned:

3.3.11.6.1.1. shall constantly monitor the alerts disclosed by the governmental incident response center on critical network security incidents and vulnerabilities;

3.3.11.6.1.2. shall constantly monitor the notifications from the National Cyber Security Center;

3.3.11.6.1.3. if necessary, shall issue an internal security alert and warning;

3.3.11.6.1.4. shall transfer the internal security alert and warning to the competent persons;

3.3.11.6.1.5. shall establish and operate the system of the obligation to report an event as specified by law, and shall keep in touch with the relevant bodies specified in separate legislation;

3.3.11.6.1.6. shall take appropriate countermeasures and responses.

3.3.11.6.2. Automatic alerts

Mechanisms shall be developed to ensure the availability of security alerts and warnings within the body.

3.3.11.7. Checking security functionality

3.3.11.7.1. The electronic information system:

3.3.11.7.1.1. shall check the set security functions on the instructions of the user authorized to check or periodically;

3.3.11.7.1.2. shall send a notification to the persons and roles determined by the body concerned, if the check reveals an error;

3.3.11.7.1.3. shall shut down the system if an abnormality is detected, shall restart the system at the discretion of the body concerned or take other countermeasures.

3.3.11.8. Software and information integrity

3.3.11.8.1. The body concerned shall use an integrity control device to detect unauthorized changes in software and information.

3.3.11.8.2. Integrity check

The electronic information system shall carry out integrity checks on specified software and information when restarting the system or following a security incident or with a specified frequency.

3.3.11.8.3. Detection and reaction

The body concerned shall incorporate the detection of unauthorized changes in the electronic information system into its security incident response procedures.

3.3.11.8.4. Automatic notification

The body concerned shall use automated means to notify specified persons and roles, if the integrity check reveals an abnormality.

3.3.11.8.5. Automatic reaction

The electronic information system shall automatically shut down or restart the system, or take other measures, if the integrity check reveals an abnormality.

3.3.11.8.6. Executable code

The electronic information system shall prohibit the use of binary or machine code which comes from an uncontrolled source, or the electronic information system does not have its source code.

3.3.11.9. Protection against spams

3.3.11.9.1. The body concerned:

3.3.11.9.1.1. shall implement protection against unwanted messages - so-called spams - at the entry and exit points of the electronic information system to detect and filter spams;

3.3.11.9.1.2. shall update protection mechanisms against spams in compliance with configuration management rules and the rules of procedure when updates appear.

3.3.11.9.2. Central management

The body concerned shall control spam protection with central settings.

3.3.11.9.3. Update

The electronic information system shall automatically update anti-spam mechanisms with their newer versions.

3.3.11.10. Input information check

The electronic information system shall check validity of specified information entry points.

3.3.11.11. Error management

3.3.11.11.1. The electronic information system:

3.3.11.11.1.1. shall generate error messages providing the information needed to correct the error; however, it does not provide any information which attackers can take advantage of;

3.3.11.11.1.2. shall make error messages available only to persons and roles determined.

3.3.11.12. Management and storage output information

The body concerned shall process and preserve output information of electronic information systems in accordance with laws, regulations and operational requirements.

3.3.11.13. Memory protection

Security settings shall be applied in electronic information systems in order to protect the memory from executing unauthorized codes.

3.3.12. LOGGING AND ACCOUNTABILITY

3.3.12.1. Logging procedures

3.3.12.1.1. The body concerned:

3.3.12.1.1.1. shall develop and document according to the requirements applicable to the body concerned, and promulgate the rules of logging procedures to the persons and roles determined in its regulation within the body concerned, which facilitates the implementation of logging and accountability policy, and the controls related thereto;

3.3.12.1.1.2. shall review and update the rule of logging procedures with a frequency specified in the rules of logging and accountability procedures or in other internal regulations.

3.3.12.2. Events that can be logged

3.3.12.2.1. The body concerned:

3.3.12.2.1.1. shall specify the events that can and shall be logged, and shall prepare its electronic information system therefor;

3.3.12.2.1.2. shall harmonize security log functions with other organizational units that require log information to increase mutual support and to provide guidance in selecting the events that can be logged;

3.3.12.2.1.3. shall examine whether the events that can be logged can be considered adequate to support fact-finding investigations following security incidents.

3.3.12.2.2. Review

The body concerned shall review and update the events to be logged with a specified frequency.

3.3.12.3. Contents of log entries

3.3.12.3.1. The electronic information system shall gather enough information in log entries to demonstrate the kind of events happened, where these events came from, and what the outcome of these events was.

3.3.12.3.2. Additional information

In log entries, the electronic information system shall also record additional, more detailed information specified by the body concerned.

3.3.12.3.3. Central management

The electronic information systems shall provide central management and configuration of the contents of log entries generated by specific system elements.

3.3.12.4. Log storage capacity

The body concerned shall provide sufficient storage capacity for logging, taking into account the logging functions resulting from the security classification.

3.3.12.5. Logging error management

3.3.12.5.1. The electronic information systems:

3.3.12.5.1.1. shall send an alert to persons or roles determined in case of a logging error;

3.3.12.5.1.2. shall execute the specified activities to be performed, thus for instance shutting down the system, overwriting oldest log entries, stopping the logging process.

3.3.12.5.2. Logging storage check

The electronic information systems shall notify the specified persons, roles and locations, if the allocated log storage space reaches a predetermined portion of the set maximum log storage space.

3.3.12.5.3. Real-time alert

The electronic information systems shall send an alert, if an event occurs that is on the list of specified error events that require a real-time alert.

3.3.12.6. Logging and reporting

3.3.12.6.1. The body concerned:

3.3.12.6.1.1. shall regularly review and analyse log entries to look for signs of improper or unusual operation;

3.3.12.6.1.2. shall notify them to the persons and roles determined.

3.3.12.6.2. Integration into processes

The body concerned shall use automatic mechanisms to integrate the examination, analysis and report of log entries into a comprehensive process, which responds to hazardous or prohibited activities and events.

3.3.12.6.3. Summary

The body concerned shall examine and associate log entries in different repositories for an assessment of the situation throughout the body concerned.

3.3.12.6.4. Integration of supervisory capabilities

The body concerned shall integrate scanning of log entries with the information on vulnerability checks, performance data, information from the supervision of electronic information systems or data or information gathered from other sources.

3.3.12.6.5. Linking to physical access information

The body concerned shall link the information from the log entries with the information obtained from the physical access control.

3.3.12.7. Log reduction and reporting

3.3.12.7.1. The electronic information system:

3.3.12.7.1.1. shall provide the ability to reduce logs and generate reports, which supports the log review, log auditing and reporting requirements to be performed on demand and the fact-finding investigations following security incidents;

3.3.12.7.1.2. may not change the original content and chronology of log entries.

3.3.12.7.2. Automatic processing

The electronic information system shall ensure that important log entries can be processed automatically.

3.3.12.8. Timestamps

3.3.12.8.1. The electronic information system:

3.3.12.8.1.1. shall use internal system clocks to generate timestamps for log entries;

3.3.12.8.1.2. shall record timestamps in log entries in a way that can be assigned to the Universal Time Coordinated - so-called UTC - or to the Greenwich Mean Time - so-called GMT -, in accordance with the timing accuracy specified by the body concerned.

3.3.12.8.2. Synchronization

The electronic information system shall compare internal system clocks with an authentic external time source with a specified frequency, and if the time difference is greater than the specified duration, the internal system clocks shall be synchronized with the authentic external time source.

3.3.12.9. Protecting log information

3.3.12.9.1. The electronic information system shall protect log information and log management tools against unauthorized access, modification and deletion.

3.3.12.9.2. Restriction of access

Only privileged users determined by the body concerned are entitled to manage log functions.

3.3.12.9.3. Physically separate saving

The electronic information system shall save log entries on a system or system element physically separated from its place of origin with a specified frequency.

3.3.12.9.4. Cryptographic protection

Cryptographic mechanisms shall be used to protect the integrity of the log information and the log management device.

3.3.12.10. Non-repudiation

The electronic information system shall provide protection against a certain person denying as regards the application us, whether an activity subject to the non-repudiation requirement has been done by such person.

3.3.12.11. Preservation of log entries

The body concerned shall retain log entries for a specified period of time complying with legal and internal information retention requirements to ensure the ex-post investigation of security incidents.

3.3.12.12. Log generation

3.3.12.12.1. The electronic information system:

3.3.12.12.1.1. shall provide the opportunity to generate a log entry for the events that can be logged determined in point 3.3.12.2;

3.3.12.12.1.2. shall provide the opportunity to persons and roles determined to choose which events that can be logged are logged to the certain elements of the electronic information system;

3.3.12.12.1.3. shall generate log entries to the events under point 3.3.12.2 with the content determined in point 3.3.12.3.

3.3.12.12.2. System-wide time-base log

The electronic information system shall compile a system-wide (logical or physical) audit log from its log entries, which also contains time conditions beyond the tolerance specified for the relationship between the timestamps of the individual entries in the review log.

3.3.12.12.3. Changes

The electronic information system shall provide the opportunity to persons and roles determined to change the logging to be performed on each system element based on selected event criteria within a specified period.

3.3.13. SYSTEM AND COMMUNICATION PROTECTION

3.3.13.1. System and communication protection procedures

3.3.13.1.1. The body concerned:

3.3.13.1.1.1. shall develop and document according to the requirements applicable to the body concerned, and promulgate the rules of system and communication protection procedures to the persons and roles determined in its regulation within the body concerned, which facilitates the implementation of the system and communication protection policy, and the controls related thereto;

3.3.13.1.1.2. shall review and update the rules of system and communication protection procedures with a frequency specified in the rules of system and communication protection procedures or in other internal regulations.

3.3.13.2. Application separation

The electronic information system shall separate functionality available to users (including user interface services) from governance functionality of electronic information systems.

3.3.13.3. Separation of security functions

The electronic information system shall separate security functions from non-security functions.

3.3.13.4. Residue information

The electronic information system shall prevent unauthorized or accidental flow of information through shared system resources.

3.3.13.5. Overload - service denial upon attack - protection

The electronic information system shall protect against overload (so-called service denial) attacks, or shall limit their impacts based on a list of denial-type attacks by introducing specific security measures.

3.3.13.6. Border defences

3.3.13.6.1. The electronic information system:

3.3.13.6.1.1. shall supervise and monitor communication at its external borders as well as at key internal borders of the system;

3.3.13.6.1.2. shall place publicly accessible system elements physically or logically in subnets, separated from the internal organizational network;

3.3.13.6.1.3. shall join to external network or external electronic information systems only through interfaces managed on border control devices located in accordance with the security architecture of the body concerned.

3.3.13.6.2. Access points

The body concerned shall limit the number of external network connections of the electronic information system.

3.3.13.6.3. External communication services

3.3.13.6.3.1. The body concerned:

3.3.13.6.3.1.1. shall operate a supervised interface to all external ICT services;

3.3.13.6.3.1.2. shall establish traffic flow rules for each supervised interface;

3.3.13.6.3.1.3. shall protect the confidentiality and integrity of the information transmitted at all interfaces;

3.3.13.6.3.1.4. shall document every exception to traffic flow rules, together with the core task supporting exceptions and the duration of the requested exception;

3.3.13.6.3.1.5. shall review the exceptions to traffic flow rules with a specified frequency, and shall remove the exceptions which are no longer justified by a direct core task.

3.3.13.6.4. Default rejection

The electronic information system shall disable network traffic and shall allow it only as an exception on its supervised interfaces.

3.3.13.6.5. Disabling shared channel usage on remote devices

The electronic information system connected to a remote device shall prevent that the device establishes local connections to the system at the same time.

3.3.13.6.6. Authenticated proxy servers

The electronic information system shall manage internal communication traffic on supervised interfaces to specified external networks using authenticated proxy servers (servers, computers or server applications that forward client requests to other servers as an intermediate element).

3.3.13.6.7. Security error condition

The electronic information system shall be in a state of error condition in the event of a malfunction of the border protection device.

3.3.13.6.8. Separation of system elements

The body concerned shall apply border protection mechanisms for the separation of those electronic information system elements which support the specified core tasks and core functions.

3.3.13.7. Secrecy of data transmission

3.3.13.7.1. The electronic information system shall protect the secrecy of information transmitted.

3.3.13.7.2. Cryptographic or other protection

The electronic information system shall apply cryptographic mechanisms against unauthorized disclosure of information during data transmission, except when the transmission is protected by another alternative physical countermeasure specified by the body concerned.

3.3.13.8. Integrity of data transmission

3.3.13.8.1. The electronic information system shall protect the integrity of the information transmitted.

3.3.13.8.2. Cryptographic or other protection

The electronic information system shall apply cryptographic mechanisms for the detection of changes in information during data transmission, if the transmission is not protected by other alternative physical measures.

3.3.13.9. Disconnection of the network

After a certain period of inactivity, the electronic information system shall disconnect the network connection when a two-way data exchange based on a work phase is completed.

3.3.13.10. Cryptographic key generation and management

3.3.13.10.1. The body concerned shall generate and manage cryptographic keys required for the cryptography applied in the electronic information system, in accordance with its internal regulations for the generation, distribution, storage, access and destruction of keys.

3.3.13.10.2. Availability

The body concerned shall create, ensure the availability of information even in the case, when cryptographic keys become inaccessible (loss, damage, destruction).

3.3.13.11. Cryptographic protection

The electronic information system shall implement standard cryptographic operations that are classified as secure in other pieces of legislation.

3.3.13.12. Collaborative IT devices

The electronic information system shall prevent remote activation of collaborative IT devices (e.g. cameras, microphones), except if the body concerned authorized it and provides a direct signal about remote activity to the users who are physically present at the devices.

3.3.13.13. Public Key Infrastructure certificates

The body concerned shall issue public key certificates according to the internal authentication system, or shall obtain public key certificates from the certification-service-providers included in the electronic signature register of the National Media and Communications Authority (NMHH).

3.3.13.14. Mobile code restrictions

3.3.13.14.1. The body concerned:

3.3.13.14.1.1. shall determine acceptable and unacceptable mobile codes and mobile code technologies;

3.3.13.14.1.2. shall introduce restrictions on use or issue implementation guidelines for acceptable mobile codes and mobile code technologies;

3.3.13.14.1.3. shall authorize, supervise and monitor the use of mobile codes within the electronic information system.

3.3.13.15. Voice over electronic information system (so-called Voice over Internet Protocol, VoIP)

3.3.13.15.1. The body concerned:

3.3.13.15.1.1. shall introduce restrictions on use or issue implementation guidelines for VoIP technologies, assessing the damage that malicious use can cause in the electronic information system;

3.3.13.15.1.2. shall authorize, supervise and monitor the use of VoIP within the electronic information system.

3.3.13.16. Secure name/address resolution services (so-called authentic source)

The electronic information system shall provide additional information on the origin and integrity of the information in addition to the authentic data for name/address resolution requests, and if it operates as part of a distributed, hierarchical directory, it also indicates the security status of progeny domains, and (if they support secure resolution services) authenticates the chain of trust between predecessor and progeny domains.

3.3.13.17. Secure name/address resolution service (so-called resolution using recursive or cache storage)

The electronic information system shall request authentication and data integrity verification, and shall execute name/address resolution responses from the authentic source.

3.3.13.18. Architecture and reserves for name/address resolution service

The electronic information systems which ensure joint name/address resolution service to a body, shall be resilient and implement internal/external role separation.

3.3.13.19. Authenticity of the work phase

The electronic information system shall protect the authenticity of work phases.

3.3.13.20. Known condition after error

After an error for specific error types, the electronic information system shall come to the designated state or to the last known state which retains system status information even in the event of an error.

3.3.13.21. Residual information protection

The electronic information system shall protect secrecy and integrity of residual information determined by the body concerned (e.g. temporary files).

3.3.13.22. Separation of processes

The electronic information system shall maintain a separate execution range for each execution process.