Declared: 20 December 2018. Time version of the regulation effective as of 1 January 2019.
The content of this document is legally binding.

COLLECTIONS OF LAWS

OF THE SLOVAK REPUBLIC

2018

362

DECREE

of the National Security Authority

of 11 december 2018,

laying down the Content of Security Measures, the Content and Structure of Security Documentation and The Scope of General Security Measures

The National Security Authority pursuant to Article 32 (1) letter c) of the Act No. 69/2018 Coll. on Cybersecurity and on Amendment and Supplementing of certain Acts (hereinafter referred to as “the Act") lays down:

Article 1
Basic Provisions

(1) This Decree regulates the content of security measures, the content and structure of security documentation and the scope of general security measures which shall be adopted by an operator of essential services pursuant to Article 3 letter l) of the Act for information systems and networks through which the essential service is provided according to Article 3 letter k) of the Act for information systems and networks whose failure or damage may cause damage or break down of providing essential services.

(2) Security measures shall be adopted on the basis of recommendations of internationally accepted cybersecurity standards or other materially similar procedures and methods being state of the art, while identifying the risks, vulnerabilities and regulatory requirements within the sector of an operator of essential services according to Annex 1 of the Act.

(3) General security measures shall be adopted and documented in the security documentation for all fields according to Article 20 (3) of the Act depending on categorization of networks and information systems, and to the extent stipulated in Articles 5 to 17.

Article 2
The Content and Structure of Security Documentation

(1) The security documentation shall contain:

a) approved security strategy of cybersecurity and security policies of cybersecurity,

b) information classification and categorization of networks and information systems,

c) documented definition of the scope and manner of compliance with all security measures; a particular content may be derived from the principles of one of the security architecture management frameworks,

d) performed cybersecurity risk analysis,

e) final report on results of the cybersecurity audit according to Article 29 of the Act.

(2) The security documentation shall be drawn up on the basis of assessment of provided essential service and thereto related

a) infrastructure of production technologies,

b) infrastructure of information and communication technologies,

c) application architecture,

d) security architecture and implemented security measures,

e) organizational structures, work roles, responsibilities and division of powers,

f) common frameworks of operational risk management,

g) organizational culture and social responsibility.

(3) The security documentation of cybersecurity may also contain

a) security standards that interpret requirements of valid security policies in specific situations, determine activities, basic rules, responsibilities and the organization of management for the purpose of supporting the compliance with security policies, and

b) security instructions that represent a summary of required steps for implementing the security policies and security standards through specific actions, and describe security configurations and provide particular, platform-related regulations to support security policies and security standards.

Article 3

Security Strategy of Cybersecurity

(1) The security strategy of cybersecurity shall identify the objectives to be achieved on the basis of the results of cybersecurity risk analysis, together with an indication of the basic principles for achieving them and the identification of powers and responsibilities for the cybersecurity management, cybersecurity risk management and the security documentation update.

(2) The security strategy of cybersecurity may be adopted separately or as one of the security policies of cybersecurity.

(3) Based on the security strategy of cybersecurity, the security policies of cybersecurity shall be adopted according to Annex 1.

Article 4

Information Classification and Categorization of Networks and Information Systems

(1) Information classification and categorization of networks and information systems according to Article 20 (2) of the Act shall be performed within the classification scheme in compliance with the structure of the information classification and the categorization of networks and information systems according to Annex 2. If the operator of essential services has own information classification and categorization of networks and information systems, the mapping for classification in the classification scheme in compliance with the structure of the information classification and the categorization of networks and information systems shall be performed according to Annex 2.

(2) The information classification and the categorization of networks and information systems shall reflect the requirements of cybersecurity throughout the lifecycle of the information, networks and information systems, particularly in the phase of

b) specification, as a definition of requirements and needs leading to decision on the establishment of the information system or any processing of the information,

c) design of the process, system or data structure,

d) system development or a method of information processing,

e) system implementation including installation, deployment, launching or a system recovery, or initialization of the information processing,

f) operation of the process, as a standard use and maintenance of a system, and information maintenance,

g) change of existing, running system, or the information processing, development and innovation of processing according to current needs of the operator of essential services,

h) replacing of the system or the information processing with a new system or process and

i) decommissioning, as termination of the information processing or putting the system out of operation.

(3) Information shall be classified irrespective of its format, storage method, systems, applications or devices in which it is located or through which the information is processed or transmitted.

(4) A graded approach shall be applied in information classification, the information with the lowest demands on confidentiality, integrity, availability and accountability, along with the quality assurance, being included in lower levels. The information shall be created, processed and stored in such a way that its quality and reliability is appropriate to its classification level.

(5) The categorization of networks and information systems shall be based on the information classification.

(6) The categorization of networks and information systems shall be performed for each network and information system by creating a list of selected networks and information system components, which identifies individual networks and information systems, their auxiliary systems and subsystems, with their security function and respective security categorization.

(7) The list of networks and information system components identifying individual networks and information systems may consist of a textual, tabular or graphical parts so that the perimeters of a selected network and information system, interfaces between defined perimeters, security functions of components to be included in the assessment of security levels and the requirements of relevant regulatory measures and technical standards or other materially similar procedures and methods for their design, creation, implementation and audit, shall be clearly defined.

(8) Networks and information systems forming perimeters between different security categories in the security system shall be assigned a higher security category.

(9) The categorization of networks and information systems takes into account that the failure of a network or an information system at any security level shall not cause the failure of a selected network and information system assigned to a security level of a higher category. Auxiliary networks and information systems and subsystems that assist the functions of selected information systems shall be assigned to an appropriate security category with regard to the categorization of a higher system.

(10) Minimum requirements for security measures depending on categorization of networks and information systems are stipulated in Annex 3.

Article 5

Security Measures for the Field pursuant to Article 20 (3) Letter a) of the Act

For cybersecurity organization purposes, at least the following principle shall apply:

a) the appointment of a cybersecurity manager who shall

1. submit proposals and report the information in the field of cybersecurity directly to the statutory body of the operator of essential services,

2. ensure the application of security measures in the cybersecurity management system,

3. be independent of the operation management and development of information technology services and

4. meet the knowledge-based standards for the position of a cybersecurity manager according to a specific legal regulation,

b) the lowest privileges, according to which each user is limited to privileges in the maximum extent required to fulfil the assigned tasks,

c) separation of responsibilities, according to which none of the users is authorized to access, modify or use the assets of the operator of essential services without authorization or identity verification,

d) compliance with and performance of independent assessment, measuring and examining the effectiveness of measures adopted for risk treatment,

e) a clear definition of powers, duties and responsibilities that form a part of the job description or a similar description of work activities.

Article 6

Security Measures for the Field pursuant to Article 20 (3) Letter b) of the Act

(1) Asset, threat and risk management shall be a process associated with financial, contractual and inventory functions to support the lifecycle management of information technologies and configuration items. The purpose of the asset, threat and risk management shall be to ensure the protection of assets according to their value.

(2) All assets related to information processing devices and information means shall be identified and the inventory of these assets shall be centrally recorded and managed.

(3) The asset management shall consist of the identification and record keeping of all

a) assets upon which the essential service providing depends,

b) supporting services through which the continuity and providing of essential services is ensured,

c) persons responsible for the asset identification and record keeping and

d) asset owners.

(4) The same protection shall not apply to all types of assets. For this purpose, assets shall be classified and categorized in accordance with the procedure stipulated in Article 4.

(5) Upon termination of employment or other similar employment relation of employees of the operator of essential services and employees of third parties, all assets in trust shall be recovered in a documented manner.

(6) The risk management shall consist of

a) vulnerability identification,

b) threat identification,

c) risk analysis and identification with respect to the asset,

d) identification of the risk owner,

e) implementation of organizational and technical security measures depending on the risks identified, including the information on which security measures shall be implemented and which security measures shall not be implemented together with the justification,

f) analysis of functional impact and

g) a regular review of the risks identified and, accordingly, updates of the security measures adopted.

(7) The risk identification shall be performed on the basis of the worst-case scenario which may occur even with a low probability. In order to determine the level of the risk identified, a set of rules shall be set up allowing to define measurable and objective risk levels for the worst-case scenarios according to standard and repeatable procedures.

(8) The risk analysis shall identify the probability of a harmful event occurrence that may be caused by abusing the existing asset vulnerability with a potential threat in connection with existing security measures and the identification of impacts in breach of the asset confidentiality, integrity or availability.

(9) The threat identification shall be based on the identification of assets and their owners and on the identification of vulnerabilities potentially affecting these assets.

(10) For the risk analysis purposes, the list of threats shall be divided into individual groups, so that it can be used generally for most assets. For individual assets, only threats relevant to a specific asset shall be assessed. Threats shall be categorized according to their origin at least as

a) intentional threats to all intentional asset-focused activities,

b) random threats to all human activities that may accidentally damage assets,

c) environmental threats to all events occurring independently of human activity.

(11) Asset, threat and risk management shall also include an analysis of functional impact, which consists of an assessment of the impact on activities of the operator of essential services caused by a crisis scenario that may affect the resources and assets supporting the processes of the operator of essential services and compromise or disrupt the continuity of the essential services they provide.

Article 7

Security Measures for the Field pursuant to Article 20 (3) Letter c) of the Act

Personnel security shall consist of at least

a) procedures for assigning a person to some of the security roles, transferring the rights, duties and responsibilities in relation to cybersecurity to another person,

b) introduction of a security awareness and education development plan to get acquainted users, administrators, persons holding one of the security roles and suppliers with security policies and ensuring their awareness-raising on a regular basis during the employment relation or other similar employment or contractual relation,

c) checking the compliance with security policies of employees, administrators, persons holding one of the security roles and suppliers,

d) evaluation of the effectiveness of the security awareness development plan for employees, administrators, persons holding one of the security roles and suppliers,

e) identifying the rules and procedures to address the cases of security policy breach caused by users, administrators, persons holding one of the security roles, and suppliers,

f) procedures allowing the transfer of rights, duties and responsibilities to other new person upon termination of the employment relation or other similar employment or contractual relation with a user, administrator, or a person holding one of the security roles,

g) procedures consisting in authorization to restrict or remove access rights and privileges in case of security policy breach,

h) giving instructions on information handling to persons who perform the activity or get acquainted with the information according to a specific legal regulation.[1])

Article 8

Security Measures for the Field pursuant to Article 20 (3) Letter d) of the Act

(1) Risks of supplier services, acquisition, development and maintenance of information systems shall be analysed in a manner according to Article 6 at the conclusion of a contract with a third party pursuant to Article 2 of the Act for the management of supplier services, acquisition, development and maintenance of information systems.

(2) The contract with a third party shall contain at least

a) duration of the contract,

b) provision on a third party commitment to comply with the security policies of the operator of essential services and declaration of consent with them,

c) provision on the obligation to protect all information provided by the operator of essential services to a third party,

d) provision on the obligation to comply with and adopt security measures by a third party,

e) particular specification and scope of security measures adopted by a third party and declaration of consent with them,

f) a specific scope of a third party activity,

g) a list of third party roles to have access to the information and data of the operator of essential services, with an obligation to notify the operator of essential services of any change in staffing; the person concerned shall sign a confidentiality agreement pursuant to Article 12 (1) of the Act,

h) provision on the scope, manner and possibility of carrying out supervisory activities and audits by the operator of essential services on third party site,

i) definition of conditions and possibilities to involve another supplier fully or partially ensuring the tasks for the operator of essential services instead of the supplier,

j) provisions on the obligation to notify the operator of essential services of a cybersecurity incident and of all facts affecting the cybersecurity,

k) provisions on the manner and form of reporting other information required by the operator of essential services to meet obligations pursuant to the Act and their definition,

---

[1]) Article 14b of Act of the National Council of the Slovak Republic No. 198/1994 Coll. on Military Intelligence.

l) provision on the manner and form of reporting all information affecting the contract,

m) provision on sanction mechanisms in case of breach of the contract,

n) provisions on terms and manner for termination of the contract,

o) a third party commitment to return, transfer or even destroy all information to which a third party has access during the contractual relation, to the operator of essential services, upon termination of the contractual relation,

p) a third party commitment to grant, provide, transfer or assign all necessary licenses, rights or consents required for ensuring the continuity of the essential service provided to the operator of essential services, upon termination of the contractual relation; the third party commitment shall remain in force after the termination of the contractual relation for a period agreed by the parties, which shall not be less than five years upon termination of the contractual relation.

(3) The contract with a third party shall contain security measures at least for the field pursuant to Article 20 (3) letters e), f), h), j) and k) of the Act.

(4) The network and information system development and acquisition of the essential service shall be carried out with regard to ensuring the compatibility with existing networks and information systems and maintaining the level of security stipulated in the security strategy.

(5) Records of all contracts concluded with a third party shall be a part of the security documentation pursuant to Article 2 (1) letter c).

Article 9

Security Measures for the Field pursuant to Article 20 (3) Letter e) of the Act

Technical vulnerabilities of information systems as a whole shall be identified through

a) a tool designed to detect existing vulnerabilities in software and parts thereof,

b) a tool designed to detect existing vulnerabilities in technical devices and parts thereof,

c) using the public and manufacturer-provided lists describing the vulnerabilities in software and technical devices.

Article 10

Security Measures for the Field pursuant to Article 20(3) Letter f) of the Act

Security management of networks and information systems shall be ensured at least by

a) management of users' access to networks and information systems according to Article 12,

b) management of secure access between external and internal networks and information systems, in particular through the use of tools for networks and information system integrity protection, secured with networks and information system segmentation; servers with services directly accessible from external networks shall be located in separate network segments; and only servers with the same security requirements, the same security class and with the similar purpose shall be in the same segment,

c) the fact that links between segments and external networks that are protected by a firewall and all connections are allowed upon the principle of the lowest privileges,

d) security measures for secure mobile connection to network and information systems and a remote access, for example in a secure way using two-factor authentication or encryption means,

e) the fact that only specified services located in authorized network segments of the computer network are allowed to network or information systems,

f) the fact that connections to external networks shall be routed through a network firewall and, depending on the environment, also through an intrusion detection system,

g) servers available from external networks secured according to the manufacturer's recommendations,

h) keeping the updated list of all input-output points on the network perimeter,

i) using automation means to identify unauthorized network connections at the perimeter with the external network,

j) blocking unauthorized connections from known addresses identified as malicious or causing known threats, if allowed by the information system settings,

k) not allowing communication and operation of applications via unauthorized ports,

l) a security monitoring system configured to record and evaluate also information about network packets at the network perimeter,

m) implementing an intrusion detection system or intrusion prevention system to identify unusual attack mechanisms or proactive blocking of malicious network traffic,

n) routing the outbound user network traffic through an authenticated server for content filtering,

o) request for two-factor authentication from each remote connection to internal network,

p) conducting regular or continuous assessments of technical vulnerabilities, in particular identifying the possible presence of malicious code of the device remotely connecting to the internal network, or the contractual guarantee including the proof of compliance with this duty.

Article 11

Security Measures for the Field pursuant to Article 20(3) Letter g) of the Act

Security management of network and information system operation shall be ensured through specified rules and procedures for

a) change management,

b) patch and update management,

c) capacity management,

d) regular backups and testing the information recovery form backups,

e) protection against malicious code,

f) software installation in networks and information systems,

g) device installation in networks and information systems,

h) recording and evaluation of operating and security records.

Article 12

Security Measures for the Field pursuant to Article 20 (3) Letter h) of the Act

(1) Management of persons' access to network and information systems shall be based on the principle that the user shall have access only to those assets and functionalities within the network and information systems that are necessary to perform the assigned tasks. For this purpose, the principles of managing persons' access to network and information systems shall be developed to define granting or revocation of users' access rights, their formal registration and keeping complete operating records of each access to network and information systems.

(2) Management of access to networks and information systems shall be based on the operating and security needs of the operator of essential services, while adopting security measures that ensure protection of the data used to log in to networks and information systems and prevent unauthorized persons from abuse of such data.

(3) Management of persons' access to network and information systems shall include at least

a) developing principles for managing access to information,

b) management of users' access,

c) users' responsibility,

d) management of access to networks,

e) access to operating system and its services,

f) access to applications,

g) monitoring of access and usage of information system and

h) management of remote access.

(4) Within the management of access to networks according to paragraph 3 letter d) above

a) every user of network and information systems shall be assigned with a unique identifier for authentication of access to the network and information systems,

b) management of users' unique identifiers including access rights and authorizations of user accounts shall be ensured,

c) a tool for user's identity management and verification prior to his activity within the network and information systems shall be used and a tool to manage access rights shall be used to control access to individual applications and data, access to read and write data, and to change authorizations, and through which the use of access authorizations (operating records) shall be recorded,

d) regular checks of access accounts and access authorizations shall be carried out to verify the compliance of approved authorizations with the actual status of authorizations and to detect and delete subsequently unused access accounts,

e) a person shall be appointed to hold responsibility for management of users' access to network and information systems and for granting and revoking the users' access rights, their formal registration and keeping complete operating records of each access to network and information systems in accordance with the relevant security policy.

Article 13

Security Measures for the Field pursuant to Article 20 (3) Letter i) of the Act

(1) Confidentiality, integrity, availability and authenticity of data within the networks and information systems through which the essential service is provided shall be ensured by encryption means, using sufficiently resistant encryption mechanisms, while encryption data protection rules for data transmission or storage within the networks and information systems shall be specified.

(2) Encryption key and certificate management system shall be ensured throughout the lifecycle of encryption keys and certificates. The encryption key and certificate management shall include at least:

a) secure handling of encryption keys and certificates,

b) generating the pseudo-random numbers and keys, setting up, distribution, insertion, modification, validity restriction, selection, storage and key destruction and certificate invalidation,

c) allowing inspections and audit.

Article 14

Security Measures for the Field pursuant to Article 20 (3) Letter j) of the Act

(1) Cybersecurity incident handling shall include at least

a) preparation and development of standards and procedures for cybersecurity incident handling,

b) monitoring and analysing the events in networks and information systems,

c) detection of cybersecurity incidents,

d) collection of relevant information on cybersecurity incidents,

e) evaluation of cybersecurity incidents,

f) handling of identified cybersecurity incidents and mitigating the consequences of detected cybersecurity incidents and

g) evaluation of methods of cybersecurity incident handling after resolving the incidents and adopting the measures or introducing new procedures to minimize the occurrence of similar cybersecurity incidents.

(2) Standards and procedures for cybersecurity incident handling shall be developed and regularly updated to address handling of cybersecurity incidents and shall contain at least

a) procedure for internal reporting of cybersecurity incidents,

b) procedure for reporting of cybersecurity incidents pursuant to Article 24 (1) of the Act,

c) procedure for handling of particular types of cybersecurity incidents and the method of their evaluation and

d) record-keeping methods of cybersecurity incidents and used approaches and resolutions.

(3) The process of cybersecurity incident detection shall be ensured through the tool for cybersecurity incident detection that enables verification and checking of data transferred within the networks and information systems and among networks and information systems.

(4) The process of collecting and evaluating the cybersecurity incidents shall be ensured through the tool for collection and continuous evaluation of cybersecurity incidents, which allows

a) collection and evaluation of information on cybersecurity incidents,

b) retrieval and aggregation of records related to cybersecurity incidents,

c) evaluation of security events to identify them as cybersecurity incidents,

d) revision of configuration and monitoring rules to evaluate security incidents in case of misidentified cybersecurity incidents.

(5) The process of cybersecurity incident handling shall be ensured through

a) assigning responsibilities and identifying procedures for handling of cybersecurity incidents,

b) establishing a process for retrieval and storage of information required to analyse cybersecurity events and cybersecurity incidents,

c) adopting measures to avert or mitigate the impact of cybersecurity incidents,

d) establishing a process for reporting of cybersecurity incidents,

e) keeping records of cybersecurity incidents, including used approaches and resolutions,

f) investigating and identifying the causes of a cybersecurity incident occurrence by updating the security policy and adopting appropriate security measures to prevent its recurrence, and

g) designation of a person responsible for reporting of cybersecurity incidents, arising or occurring within the network or information system of the essential service, to the Cybersecurity Single Information System.

(6) Cybersecurity incident records shall also include information identifying a cybersecurity incident such as location, hostname, MAC addresses, IP addresses, identification data of all devices and persons involved, and the date and time of data manipulation and delimitation of the affected data storage in order to use them as evidence or a means of proof.

Article 15

Security Measures for the Field pursuant to Article 20 (3) Letter k) of the Act

(1) Monitoring of networks and information systems security shall be carried out through implementation of a central tool for recording the activities of networks and information systems and their users, ensuring a security supervision of networks and information systems through recording the operation of such networks and information systems, at least to the extent of

a) central network elements and servers,

b) services accessible to external networks and

c) critical internal servers and services.

(2) Tool for recording the activities of networks and information systems and their users that enables creating operation records, shall record at least

a) activities in the form of creating, reading, updating or deleting of protected and strictly protected information and data or other information assets therein,

b) initiation of a connection to the network or information system and its acceptance or rejection by logging at least the date and time of the activity, identifying the technical means within which the activity is recorded, identifying the person and source through IP address,

c) granting, modification, or revocation of user's access rights, including adding a new user or a group of users, changing the user's authorization level, changing the firewall policy, or changing the password,

d) automatic system warning or error reports,

e) detected suspicious or malicious activities and

f) other information necessary to assess the severity of a cybersecurity incident in connection with the criticality of the service or device and the correct date and time, and the time zone used.

(3) Operating records shall be secured at least in a way that

a) are readable only by persons authorized to analyse them,

b) prevent the record from being overwritten or deleted,

c) records transferred or rerouted from the original source device to the security monitoring system are rerouted through secure channels or through a dedicated management network,

d) are kept for a period appropriate to the category of the information system.

(4) Monitoring of the operating records, their evaluation and reporting of a suspicious activity shall be the responsibility of the authorized employee of the operator of essential services or of a third party employee, if such activity is entrusted to the third party.

(5) The compliance of networks and information systems of essential services with the requirements ensuring the cybersecurity of these networks and information systems, the monitoring of the effectiveness of security measures and the evaluation of the security documentation being up-to-date shall be determined through a cybersecurity audit.

Article 16

Security Measures for the Field pursuant to Article 20 (3) Letter l) of the Act

(1) The physical security of networks and information systems shall be provided at least through

a) location of network and information systems in an area where the network and information systems, or at least the most important components thereof, are protected from the adverse natural and environmental impacts, possible consequences of technical infrastructure failures and the physical access of unauthorized persons (hereinafter referred to as “secured area”),

b) protection of the secured area by physical means, in particular walls, mechanical barrier devices, technical security devices, such as electrical security alarm devices, access control systems or camera systems,

c) ensuring that there are no facilities in the vicinity of the secured area that may compromise the network and information systems located in that secured area, in particular sewerage, water mains, flammable or other similar materials,

d) elaboration, implementation and monitoring of compliance with the rules for work in the secured area,

e) ensuring the protection against power outage in those parts of the network and information systems that require continuous operation and ensuring that such outages do not occur,

f) assuring that the backup capacities of network and information systems ensuring the availability, functionality or replacement of the network and information systems exist, and are located in the secured area in a safe distance from the secured area being backed up,

g) ensuring that the operation, use and management of the network and information systems comply with internal rules and contractual obligations,

h) policy that bans leaving physical documents unattended and requires locking computers prior to leaving the workplace.

(2) Organizational arrangements for the physical security of networks and information systems shall be ensured at least through the development, implementation and monitoring of compliance with the rules for

a) maintenance, storage and records of technical components of networks and information systems and devices of networks and information systems,

b) use of networks and information systems devices for other purposes than those intended,

c) use of networks and information systems outside the secured areas,

d) deletion, decommissioning and disposal of networks and information systems devices and all types of relevant backups,

e) physical transfer of technical components of networks and information systems or devices of networks and information systems outside the secured areas,

f) handling of the system documentation and storage media to prevent unauthorized disclosure, removal, damage or modification,

g) dimensioning and physical parameters of networks and hardware that directly or indirectly affect the maximum allowable network and information system's downtime.

Article 17

Security Measures for the Field pursuant to Article 20 (3) Letter m) of the Act

(1) Operator of essential services shall determine the requirements to ensure the continuity of cybersecurity management when a cybersecurity incident occurs.

(2) The management of the process continuity shall consist of at least

a) development of a strategy and contingency plans to ensure the availability of the network and information system after a breach or failure as a result of a cybersecurity incident, based on an analysis of the impact of the cybersecurity incident on the essential service,

b) assigning adequate financial, material, technical and personnel resources to ensure the management of operation continuity,

c) specification of a communication plan to comply with emergency and recovery plans, together with contact details, roles and responsibilities to comply with emergency and recovery plans after a cybersecurity incident,

d) specification of a target time for recovery of individual processes, network and information systems and applications, in particular by determining the operation recovery time after which the lowest level of providing the essential services is restored after a cybersecurity incident,

e) identification of a target point for recovery of individual processes, network and information systems of the essential service and applications, in particular by specifying the lowest level of providing the service which is sufficient for use, operation and management of the network and information systems and for maintaining the continuity of the essential service,

f) testing and evaluation of respective processes for management of operation continuity and implementation of measures to increase the resilience of networks and information systems of the essential service,

g) identification of disaster recovery plans and backup procedures for the network and information systems recovery after its breach or failure as a consequence of a cybersecurity incident.

(3) Backup procedures for networks and information systems recovery after its breach or failure as a consequence of a cybersecurity incident shall include at least

a) frequency and extent of its documentation and approval,

b) appointment of a person responsible for backups,

c) time range, identification of data scope, backup data medium and the requirement to keep the backup documentation,

d) requirement to locate backups in a secured access control environment,

e) requirement to ensure the encryption of backups containing assets classified as protected and strictly protected,

f) requirement to carry out a regular verification of backups, testing the backup recovery and practising introduced contingency plans at least once a year.

Article 18
Effect

This Decree shall come into force on 1 January 2019.

Jozef Magala

Annex No. 1 to Decree No. 362/2018 Coll.

CYBERSECURITY STRATEGY

A: Structure of Cybersecurity Strategy

The cybersecurity strategy shall contain at least the identification of

1. security objectives from the point of view of cybersecurity,

2. manner for security objectives evaluation, the criteria for assessing the achievement of security objectives, the manners for continuous assessment of their adequacy and the manners for checking the procedures used for achieving the security objectives,

3. the tasks of the statutory body of the operator of essential services in ensuring the cybersecurity and the declaration of commitment to support the cybersecurity,

4. general and specific responsibilities and obligations in the field of cybersecurity and the identification of relevant security roles necessary for the management of cybersecurity, including the identification of the scope of activities, competences and tasks; the division of roles into managing, executive and auditing ones, whilst the managing role is directly carried out by the operator of essential services and the auditing role is incompatible with all other roles,

5. basic framework for asset management pursuant to Article 6, on which the operation of networks and information systems depends,

6. basic framework for risk management pursuant to Article 6 in connection with the assets on which the operation of networks and information systems depends and the identification of security measures according to areas pursuant to Article 20 (3) of the Act depending on risks identified,

7. extent and periodicity of cybersecurity status validation through a cybersecurity audit, including the assessment of the compliance of the security strategy and security policies with the requirements of the Act, other generally binding legislation, internal regulations and contractual obligations,

8. the procedure and responsibilities for revising the security documentation approved by the operator of essential services, including the periodicity of regular revisions and updates thereof after any change affecting the security documentation, as well as for reasons of extraordinary revisions.

B: Structure of Cybersecurity Policy

Security policies	**Related security standards**
1. Security organization	– Management of security architecture – Cybersecurity managemen system – Identity and access control management – Privileged access control – Security monitoring and management of security records
2. Security risk management	– Testing and security certification of systems – Methodology of impact assessment on protection of personal data – Methodology of risk assessment – Physical security and environment security – Security incident handling
3. Information asset management	– Information classification and network categorization – Record Retention Rules and Record Retention Plan
4. Rules of conduct and best practices	– Remote work and mobile device usage – Management of personnel security – Communication rules
5. Management of supplier relations	– Management of supplier services – Acquisition of information systems
6. Development and maintenance management in the field of information and communication technologies	– Development and testing of the information systems – Procedures of information systems maintenance – Management of technical vulnerabilities and patch management
7. Management and operation of information and communication technologies	– Rules for interconnecting the systems and electronic information transfer – Network security management – Infrastructure change management – System and service capacity management – Encryption measures management
8. Compliance management	– Cybersecurity audit – Processing of personal data and classified information – Providing assistance to third parties
9. Management of process and operation continuity	– Plans for continuity of operating activities – Emergency recovery plans – Methodology of information backup and recovery

Annex No. 2 to Decree No. 362/2018 Coll.

CLASSIFICATION SCHEME

A. Criteria for Information Classification

Classification levels

Classification levels shall describe the sensitivity of information, data or other related information assets (hereinafter referred to as "information assets") in terms of breach of their confidentiality, integrity and availability and shall reflect the importance or value of these assets to the processes of the operator of essential services.

1. In terms of confidentiality the classification levels of information assets shall be defined as

a) **public** information assets intended for the public that are obtainable from public sources or from information prepared for this purpose or are reclassified by the owner from another level and include, for example, information from the media, obligatorily published information or generally available information,

b) **internal** information assets that are used and accessible to all users within the organization of the operator of essential services, regardless of their work role; disclosure of these assets to third parties shall require the approval of the owner of the information,

c) **protected** information assets that are used and accessible only to specified groups of authorized persons and whose unauthorized detection, disclosure or destruction may have a negative impact on the providing of the service of the operator of essential services; access to data classified as "Protected" shall be regulated by the "need-to-know" principle and by the principle of the "lowest privileges" and shall be solely limited to pre-defined and approved departments or other clearly defined groups of persons; third parties shall have access to these data only in necessary and clearly defined cases approved by the owner,

d) **strictly protected** information assets that are used and accessible only to particular selected users of the operator of essential services and whose unauthorized detection, disclosure or destruction may have, with a high probability, a negative impact on the providing of the essential service; access to data classified as "Strictly Protected" shall be regulated by the "need-to-know" principle and by the principle of the "lowest privileges" and shall be solely limited to particular, pre-defined and approved persons; third parties shall have access to this data only in necessary and clearly defined cases approved by the owner or according to provisions of specific legal regulations.

If the information asset is not explicitly classified, it shall be considered internal.

2. In terms of integrity, the classification levels of information assets shall be defined as

a) **low** including information assets whose fault or inaccuracy shall not considerably compromise the essential service provided,

b) **medium** including information assets that are relevant to the activities of the operator of essential services and whose fault or inaccuracy may have an impact on the continuity of the essential service provided, strategic area, market and operational risks,

c) high including selected key information assets that are critical to the activities of the operator of essential services and whose fault or inaccuracy shall immediately compromise the essential service provided and associated activities thereof, and the reputation of the operator of essential services.

3. In terms of availability, the classification levels of information assets shall be defined as

a) **low** including information assets of the operator of essential services whose failure shall not considerably compromise the service provided or for which alternative procedures shall exist,

b) **medium** including information assets that are relevant to the activities of the operator of essential services and whose failure may have an impact on the continuity of the essential service provided, strategic area, market and operational risks,

c) **high** including selected key information assets that are critical to the activities of the operator of essential services and whose failure shall immediately compromise the essential service provided and associated activities thereof, and the reputation of the operator of essential services.

Basic Rules for Information Classification

1. Each classified information shall be assigned a classification level of confidentiality, a classification level of integrity and a classification level of availability.

2. The security information, settings, procedures, directives and other acts concerning the asset management shall be classified at the same or higher classification level as the information assets whose management they describe.

3. The operator of essential services may classify particular information assets to a higher level within its scope of activities.

4. The operator of essential services who has already performed the classification of information according to another standardization method shall conduct a survey of classification levels pursuant to this Annex for the information classification.

B. Criteria for Categorization of Networks and Information Systems

Category I shall include information assets within the scope of activities of the operator of essential services,

a) whose compromise does not have any negative impact on the essential service provided,

b) which are classified in terms of confidentiality as public or as internal, if justified,

c) which are classified in terms of availability as low or as medium, if justified,

d) which are classified in terms of integrity as low or as medium, if justified,

e) where there is no requirement to identify the responsibility for users' activities or

f) where it is not necessary to carry out inspection activities.

Category II shall include information assets within the scope of activities of the operator of essential services,

a) whose compromise may cause a cybersecurity incident of level I,

b) which are classified in terms of confidentiality as internal, protected or, as strictly protected, if justified,

c) which are classified in terms of availability as medium or as high, if justified,

d) which are classified in terms of integrity as medium o as high, if justified,

e) where it is necessary to identify the responsibility for critical activities, in particular the activities of privileged users,

f) where it is necessary to carry out inspection activities,

g) forming basic registers and / or reference registers,

h) ensuring the creation and management of agendas not belonging to security category I,

i) that are agenda information systems,

j) that are specialized portals, or

k) which are necessary for the decision-making of the state authority.

Category III shall include information assets within the scope of activities of the operator of essential services,

a) whose compromise may cause a cybersecurity incident of levels II and III,

b) which are classified in terms of confidentiality as strictly protected,

c) which are classified in terms of availability as high,

d) which are classified in terms of integrity as high,

e) where it is necessary to conduct an audit of activities of all users,

f) through which the essential service is provided and whose failure or damage shall cause damage or outage of the providing of essential services,

g) that are defined as classified information or secrecy pursuant to a specific legal regulation[2])

h) which are necessary and required in terms of performing the tasks regarding the state defence and security, or

i) which is the central public administration portal.

---

[2]) For example Act No. 215/2004 on Protection of Classified Information and on Amendment and Supplementing of some Acts, as amended, Articles 17 through 20 of the Act No. 513/1991 Coll. Commercial Code, Article 39 of Act of the National Council of the Slovak Republic No. 323/1992 Coll. on Notaries and Notarial Activity (Notarial Order), as amended, Act No. 483/2001 Coll. on Banks and on Amendment and Supplementing of some Acts, as amended, Article 23 of Act No. 586/2003 Coll. on Advocacy and on Amendment and Supplementing of Act No. 455/1991 Coll. on Trade Business (Trade Act), as amended by Act No. 297/2008 Coll., Articles 24 and 25 of Act No. 576/2004 Coll. on Healthcare, Healthcare-Related Services and on Amendment and Supplementing of some Acts, as amended, Article 11 of Act No. 563/2009 Coll. on Tax Administration (Tax Procedure Code) and on Amendment and Supplementing of some Acts, as amended, Article 10 of Act No. 324/2011 Coll. on Postal Services and on Amendment and Supplementing of some Acts.

Annex No. 3 to Decree No. 362/2018 Coll.

MINIMUM REQUIREMENTS FOR SECURITY MEASURES DEPENDING ON CATEGORIZATION OF NETWORKS AND INFORMATION SYSTEMS

The table shows the minimum requirements for security measures for each category of networks and information systems that can be tightened up on individual assets by the operator of essential services.

Security measure for	**Category I**	**Category II**	**Category III**
The field pursuant to Article 20(3) letter a) of the Act	Recommended	Recommended	Mandatory
The field pursuant to Article 20(3) letter b) of the Act	Recommended	Mandatory	Mandatory
The field pursuant to Article 20(3) letter c) of the Act	Recommended	Mandatory	Mandatory
The field pursuant to Article 20(3) letter d) of the Act	Recommended	Mandatory	Mandatory
The field pursuant to Article 20(3) letter e) of the Act	Recommended	Mandatory	Mandatory
The field pursuant to Article 20(3) letter f) of the Act	Recommended	Mandatory	Mandatory
The field pursuant to Article 20(3) letter g) of the Act	Recommended	Mandatory	Mandatory
The field pursuant to Article 20(3) letter h) of the Act	Recommended	Mandatory	Mandatory
The field pursuant to Article 20(3) letter i) of the Act	Recommended	Recommended	Mandatory
The field pursuant to Article 20(3) letter j) of the Act	Mandatory	Mandatory	Mandatory
The field pursuant to Article 20(3) letter k) of the Act	Recommended	Mandatory	Mandatory
The field pursuant to Article 20(3) letter l) of the Act	Recommended	Recommended	Mandatory
The field pursuant to Article 20(3) letter m) of the Act	Recommended	Mandatory	Mandatory