Pursuant to Article 7, Paragraph 4 of the Law on Information Security ("Official Gazette of the Republic of Serbia", issue No. 6/16) and Article 42, Paragraph 1 of the Law on Government ("Official Gazette of the Republic of Serbia", issue No. 55/05, 71/05 - correction, 101/07, 65/08, 16/11, 68/12 – harmonized version, 72/12, 7/14 – harmonized version and 44/14),

The Government hereby adopts the

# REGULATION

## On More Detailed Regulation of Measures of Protection of Information and Communication Systems of Special Significance

### Subject of Regulation

Article 1

This Regulation shall regulate in more detail measures of protection of information and communication systems of special significance (hereinafter referred to as: measures of protection).

### Establishment of Organizational Structure, with Determined Tasks and Responsibilities of Employees, that Shall Realize Management of Information Security within Operators of ICT Systems of Special Significance

Article 2

The operator of the ICT system of special significance (hereinafter referred to as ICT system operator) shall be under obligation to determine, within the framework of the organizational structure, in compliance with the nature, scope and complexity of business operations, tasks and responsibilities of employees with the objective of managing information security.

The ICT system operator shall determine, within the framework of organizational structure, tasks and responsibilities of employees for protection of information wealth, i.e. assets and property for surveillance over business processes of significance for information security, for the management of risks in the area of information security, as well as for the tasks envisaged under procedures in the area of information security.

The division of responsibilities to employees should be performed in such a manner to prevent unauthorized or unintentional change, damaging or abuse of assets, i.e. information wealth of the ICT system operator, as well as to prevent access, changing or use or assets in the absence of an authorization and without records of that.

The ICT system operator shall establish procedures of for the purpose of monitoring activities, audit and supervision within the framework of managing information security.

In the course of determination of responsibilities of employees, it is necessary also to envisage responsibility for reporting to competent authorities on incidents in the ICT system, in compliance with regulations.

The ICT system operator shall determine procedures of communication with other institutions in case of an incident with the objective of timely reporting, i.e. resolution of the onset security incident.

### Achieving Security of Working Remotely and Using Mobile Devices

Article 3

The ICT system operator who is, within its system, allowing work remotely and use of mobile devices shall be under obligation to establish and maintain security of working remotely and of using mobile devices, taking into account the risks that may exist due to inadequate use of mobile devices.

The ICT system operator shall be under obligation to define requirements and constraints for working remotely so that the security of the ICT system is not jeopardized, wherein the ICT system operator shall take into account the physical security of the location and the surroundings from which remote work is being performed, requirements for security of communication between the ICT system of the operator and the location from which remote work is performed, prevention or reducing to the necessary minimum the processing and storing of information on personal devices of persons who are working remotely, prevention of unauthorized access, requirements for using the local network and wireless network services, requirements for protection from malware and other measures that are necessary for security in working remotely.

When using mobile devices, protection of data of interest for the ICT system must be ensured, and risks must be mitigated in using mobile devices in unprotected environments (public places, networks with unknown or insufficient protection and similar), wherein the ICT system operator shall take into account the following:

1) records of mobile devices;
2) measures of physical protection of mobile devices (from destruction, damage, loss, or unauthorized access to devices and data of interest for the ICT systems operator);
3) constraints for installation and updating of the software;
4) installation of adequate software for mobile devices and their regular updating;
5) constraints for using information society services that would jeopardize information security of the ICT system;
6) control of access to the mobile device and data on it;
7) cryptographic techniques;
8) protection from viruses and other malware;
9) remote handling of the mobile device in case of an incident by an authorized person of the ICT system operator, through which it is possible to perform irrevocable deletion of data and prevention of continued use of the device;
10) establishing and maintaining a reserve copy (backup) of data;
11) facilitating secure use of internet services and applications.

If the ICT system operator allows in his system use of private mobile devices, it shall be under obligation to ensure the requirements referred to in Paragraph (3) of this Article and undertake measures with the objective of separating the private from business-related use of those devices.

**Ensuring that Persons Using ICT System, i.e. Managing ICT System Are Trained for Tasks They Are Performing and Understand Their Responsibility**

Article 4

The persons who are managing the ICT system, i.e. employed persons who are using the ICT system must have an adequate level of education and capacities, awareness of significance of the tasks they are performing and their responsibility which is determined under the contract and other enactments.

In order for the persons who are using the ICT system, i.e. managing the ICT system to understand their responsibilities, the ICT system operator shall train the employees on the importance of information security of the ICT system, measures and procedures for protection of the ICT system and their obligations.

The ICT system operator shall be under obligation to initiate appropriate proceedings against persons responsible for disrupting the security of the information system.

**Protection from Risks that Onset in Changes of Tasks or Termination of Work Engagement of Persons Employed with ICT System Operator**

Article 5

The ICT System operator shall be under obligation to commit, in a contract or another enactment, the employed persons or persons engaged on other grounds that, after the termination or change of work engagement they do not disclose any confidential or other information that is of significance for information security of the ICT system. Duties and obligation that remain valid even after the termination of engagement should be contained in the terms of the contract with the employed person, i.e. person engaged on another grounds.

**Identification of Information Wealth and Determination of Responsibility for Their Protection**

Article 6

The ICT system operator shall be under obligation to identify and classify information wealth, i.e. assets and property, with which development, processing, storing, transfer, deletion and destruction of data in the ICT system are being performed, to perform an inventory of information wealth, i.e. assets and property, and to establish, maintain and regularly update their records.

The ICT system operator shall eb under obligation to perform the classification under Paragraph 1 of this Article according to the degree of sensitivity and critical nature, taking into account potential consequences of disrupting confidentiality, integrity and availability of wealth, to apply that classification in a principled manner, as well as to ensure an adequate level of protection of that wealth in compliance with that.

For any information wealth, i.e. asset and property, it is necessary to assign a person in charge of their protection.

**Classification of Data for that Level of Their Protection Matches Significance of Data in Compliance with Principle of Risk Management under Law on Information Security**

Article 7

The ICT system operator shall determine the scheme of data classification according to which data are being classified, taking into account that sensitivity, importance of data, damage that may onset doe to unauthorized disclosure, change or deletion of data and regulations that regulate the issues of data protection (on confidential data, business secret, data on persons etc.).

The ICT system operator shall be under obligation to define a corresponding set of procedures for acting, processing, warehousing and transfer of data in compliance with the data classification scheme referred to in Paragraph 1 of this Article.

The measures of protection of data that are, in compliance with the law that regulates the area of data confidentiality, characterized as confidential, shall be determined in compliance with regulations that regulate this area.

The selection and the level of application of measures for data protection shall be based on risk assessment, the necessity of risk prevention and elimination of consequences of risk that has manifested, including all types of irregular circumstances.

## Protection of Data Carriers

Article 8

The ICT system operator shall be under obligation to ensure prevention of unauthorized disclosure, modification, removal or destruction of information and contents that are kept on data carriers, in such a manner that it shall ascertain and apply procedures for management of data carriers in compliance with classification referred to in Article 7 of this Decree.

When defining procedures and acting with data carriers, one should envisage irrevocable deletion of data, in case of expiry of deadlines for their keeping and once they are no longer necessary, the procedure for approving the data carriers to be taken our from the premises of the ICT system operator, keeping of data carriers in a secure location, using cryptographic techniques for data protection when that is envisaged under regulations, i.e. in other cases when such a type of protection is necessary, ensuing a secure transfer of data on a new data carrier, keeping backup copies on separate data carriers and other measures and procedures for protection of data carriers.

The ICT system operator should envisage procedures for secure decommissioning and destruction of data carriers once they are no longer needed, and they should reduce to the minimum level the risk of data being accessed by unauthorized persons.

Data carriers should be protected from unauthorized access, abuse or damage in transport, by ensuring reliable transport and reliable persons to transport data carriers and ensuring adequate packaging with the objective of physical protection in transport.

The ICT system operator shall determine for which data, in compliance with the data classification scheme, records would be kept on the use of data carriers and procedures undertaken in connection with protection of data and data carriers.

## Constraints in Access to Data and Means for Data Processing

Article 9

Constraints in access to data and means for data processing shall imply definition of precise rules of access, in such a manner to define who has the right to access what and which are the constraints to accessing data and means for data processing, taking care of the specificities of data and equipment and responsibilities and work-related duties of persons who are accessing data and equipment.

Constraint to access implies hardware, i.e. software constraint to accessing data and means for data processing, including also physical constraints to accessing data and means.

Constrains to access shall be performed in compliance with the classification of data under Article 7 of this Decree.

The ICT system operator should ensure access to the network and network services only to persons who have authorizations for use.

**Approving Authorized Access and Prevention of Unauthorized Access to ICT system and Services Being Performed by ICT System**

Article 10

The ICT system operator shall be under obligation to envisage a procedure for approval and revocation of authorized access to the ICT system and services being provided by the ICT system, in such a manner that it shall envisage requirements for approval and revocation of authorized access, checking of adequacy of the approved level of access and awarding the unique identification designation for the person to whom access is being approved.

The ICT system operator shall keep records on awarded and revoked designations, determine requirements to using the common identification designation in cases in which that is necessary, define the manner and conditions for preventing and eliminating unique identification designations, as well as requirements for awarding and using administrator rights.

Persons to whom authorized access is approved shall be facilitated to access on the basis of data for authentication (password, crypto graphic keys, data stored on tokens etc.).

Awarding and using administrator rights of access should be constrained and controlled.

The ICT system operator shall be under obligation to ensure a mechanism for revoking access rights in cases of change of a job, termination of labor relation, and, if necessary, in other cases.

**Determination of Responsibility of Users for Protection of Own Means of Authentication**

Article 11

The ICT system operator shall prescribe the manner of authentication of persons to whom access to the system is approved, i.e. users.

A person who is approved authorized access, i.e. a user, must commit not to disclose his data for authentication.

The ICT system operator shall envisage ways of creating and storing data for authentication which ensure a high degree of security and protection from disclosure on the part of other persons.

The ICT system operator shall envisage the obligation of changing the data for authentication in case the data are discovered, or there is increased danger of their discovery.

**Envisaging Appropriate Use of Crypto Protection in Order to Protect Confidentiality, Authenticity i.e. Integrity of Data**

Article 12

For the purpose of protection of confidentiality, authenticity and integrity of data, the ICT system operator should consider the use of appropriate measures of crypto protection, taking into account the sensitivity of information that should be protected, business processes that are being undertaken, the level of required protection, implementation of cryptographic techniques applied, and management of cryptographic keys.

The management of cryptographic keys shall cover their entire life cycle, including the generating, storing, archiving, takeover, allocation, revocation and destruction of keys.

The ICT system operator should pay special attention to protection of means for crypto protection from all forms of compromising.

**Physical Protection of Facilities, Spaces, Premises, i.e. Zones in which Means and Documents of ICT Systems Are Located and Data Are Being Processed in ICT System**

Article 13

The ICT system operator shall be under obligation to prevent unauthorized physical access to facilities, spaces, premises i.e. security zones in which the means and documents of the ICT system are located, and data are being processed in the ICT system.

In case special regulations do not envisage the obligation of establishing security zones, the ICT system operator can envisage measures of physical and technical protection of premises in which means and assets of the ICT system are located and in which data are being processed in the ICT system, such as installation of alarm devices, control of entry with obligatory wearing of visible identification throughout the stay and other that ensure physical and technical protection.

The ICT system operator shall be under obligation to envisage and apply measures of physical protection in case of elements, malware attacks, accidents or intentional destruction of facilities, premises, means and documents of the ICT system.

**Protection from Losses, Damage, Theft or Other Form of Jeopardizing Security of Assets Comprising ICT System**

Article 14

The ICT system operator shall be under obligation to protect the assets that comprise the ICT system from losses, damages, theft or another form of threat upon security.

With the objective of protection of assets, the ICT systems operator must take case of positioning the means to secure places, eliminating unnecessary access into the space in which they are located, perform regular checks of protection of the means from theft, fire, electromagnetic radiation and other threats and monitor the conditions in the environment (temperature, humidity etc.) that could have a negative impact on the functioning of the means.

The means should be protected in case of a disruption in distribution of electricity, communication capacities, water, gas, ventilation through ensuring alternative solutions that facilitate continued operations of the ICT system.

Dislocation of property of the ICT system can be performed only pending prior approval of the authorized person, and upon applying security mechanism, taking into account different risks in the course of operating outside of the premises of the organization.

**Ensuring Correct and Secure Functioning of Data Processing Means**

Article 15

With the objective of ensuring correct and secure functioning of means for data processing, the ICT system operator shall define procedures for handling the means that shall relate to initiation and completion of access to the information system, making of backup copies, maintenance of equipment, handling of data carriers, control of access into premises with server infrastructure, communication equipment and systems for data storage, as well as in cases of dislocation of parts of the ICT system.

The ICT system operator shall establish procedures for acting in case of any changes in organization, business processes, means for processing information and on systems that have

impact on the security of information and envisage responsibilities for implementation of defined procedures.

The ICT system operator shall continuously oversee and check the functioning of the means for data processing and envisage future changes that could affect the security of the ICT system and, in compliance with that plan corresponding measures.

The ICT system operator must separate environments for development, testing and operational work, in order to reduce the risks of unauthorized access or changes in the work environment.

**Protection of Data and Means for Data Processing from Malware**

Article 16

Protection of data and means for data processing should cover measures for detecting malware and for removing damages caused by malware, including corresponding controls for system access, prevention of introduction and running of malicious software, prevention of access to risky websites, continuous updating of software for detecting malware, managing vulnerabilities and checks of the ICT system, implementation of procedures, as well as raising awareness of risks from consequences of operations of malware.

**Protection from Loss of Data**

Article 17

Protection from loss of data shall be achieved through regular development of backup copies of data, software and system through corresponding means for making backup copies.

The ICT system operator shall define the duration of keeping and protection of backup copies, the scope and frequency of backup copies, secure location of keeping backup copies, ensure physical protection of backup copies and protection from external influences, check data carriers in order to ensure their correct functioning and reliability in compliance with the plan for making backup copies.

The ICT system operator shall perform the making of backup copies which should cover all systemic information, applications and data that are necessary for recovery of the entire system in case of onset of consequences caused by irregular circumstances.

**Keeping Data on Events that Could Be of Significance for ICT System Security**

Article 18

The ICT system operator should ensure that records (logs) are formed in the ICT system on events relating to activity of users, errors and events relating to information security, and they must be stored and regularly checked.

The means for logging and the logs should be protected from unauthorized access and change.

Within the framework of the ICT system activities shall be logged of the administrator and user and they shall be regularly re-examined for protection purposes.

With the objective of ensuring the reliability of the logs, the time in all the sub-systems of the ICT system must be synchronized mutually, as well as with the referential correct time.

## Ensuring the Integrity of Software and Operating Systems

Article 19

The ICT system operator shall envisage and implement procedures that ensure control of integrity of installed software and operating systems, updating of software and operating system by the authorized administrator, i.e. authorized person, application of system for control of software configuration, establishment of options for return to previous condition before implementation of changes in the system, keeping of previous versions of the software in case of unexpected situations and other measures with the objective of reducing risk from damage to software and operating systems.

## Protection from Abuse of Security Weaknesses of the ICT System

Article 20

With the objective of protection of ICT system from abuse of security weaknesses, the ICT system operator shall perform analysis of the ICT system and determine the degree of exposure of the ICT system to potential security weaknesses, and, in compliance with that, undertake corresponding measures that relate to elimination of recognized weaknesses or application of other types of protection of the ICT system.

The ICT system operator prevents unauthorized installation of software on devices that could lead to exposure of the ICT system to security weaknesses.

## Ensuring that Activities on ICT System Audit Have Least Possible Impact on System Functioning

Article 21

In the course of implementation of ICT system audit, the ICT system operator must ensure that the audit has the least possible impact on system functioning, in such a manner that it shall plan adequate time for implementation of the audit and the sequence of activities that shall not disrupt business processes of the ICT system operator.

## Protection of Data in Communication Network Including Devices and Lines

Article 22

With the objective of protection of data in communication networks, devices and lines, their control and protection from unauthorized access is being performed, wherein it is envisaged to establish procedures and responsibilities for management of network equipment, responsibility for network operations, special controls for protection of confidentiality and integrity of data that pass through public or wireless networks.

The ICT system operator shall regularly check whether there is adequate security of network services.

The ICT system operator can, with the objective of special protection of individual ICT services, perform segmentation of the network with the objective of isolation of those services and limit access to authorized persons only.

The lines for power supply and communication cables that transfer data or that represent support to information services should be protected from wiretapping, theft, disruption or damaging.

**Security of Data Being Transferred Inside ICT system Operator, as well as between ICT System Operator and Persons outside of ICT System Operator**

Article 23

Protection of Data that are being transferred through communication means within the ICT system operator, between the ICT system operator and persons outside of the ICT system operator shall be ensured by establishing procedures and adequate controls.

The procedures shall envisage protection from wiretapping, modification, incorrect addressing and destruction of data, detection and protection from malware, potential use of cryptographic techniques and other adequate measures.

When the transfer of data is being performed between the ICT system operator and persons outside of the ICT system operator, agreements can be concluded on data transfer and agreements on confidentiality or nondisclosure that contain provisions on security of data transfer.

In the case referred under Paragraph 3 of this Article, transfer of data on persons shall require fulfilment of requirements envisaged under the law that regulates protection of data on persons.

**Issues of Information Security within Management of All Phases of ICT System Lifecycle i.e. Parts of System**

Article 24

Requirements for information security must be met in all the phases of the ICT system lifecycle, i.e. all the parts of the system, which implies the phase of project design of the ICT system, establishment of a new or changing of an existing ICT system, i.e. parts of the system, and procurement of products necessary for the functioning of the ICT system.

Establishment of a new ICT system, i.e. changing an existing one, shall encompass the implementation of the procedure of documenting, definition of requirements for information security, checking of fulfilment of the requirements, controlling and managing the procedure of introduction of a new, i.e. changing of the existing ICT system.

Requirements for information security must also be met when transfer of information is being performed through public communication networks and when applicative services are used through public communication networks.

When entrusting activities in connection with the ICT system to third parties, it shall be necessary to the ICT system operator to oversee and monitor activities on ICT system development.

**Protection of Data Used for Requirements of Testing ICT Systems i.e. Parts of Systems**

Article 25

For the requirements of testing ICT systems, i.e. parts of the system, the ICT system operator shall use data that are not sensitive, which it shall protect, keep and control in the corresponding manner.

If confidential information, i.e. personal data are being used for testing needs, it shall be necessary to use them and protect them in compliance with regulations and authorizations.

**Protection of Means of ICT System Operator that Are Accessible to Service Providers**

Article 26

The ICT system operator shall envisage in its procedures the level of accessibility and the type of information and means that can be accessed by service providers, the ways of accessing information and means and supervision over access.

The ICT system operator should identify and establish procedures for information security that specifically deal with access to information on the part of service providers within the organization.

Obligations of service providers in connection with information and means that are accessible to service providers of the ICT system operator shall be regulated under an agreement between the ICT system operator and the service providers, whose provisions shall ensure an adequate level of protection of information and means, in compliance with regulations and technical standards.

The ICT system operator shall be under obligation to ensure that the service provider performs entrusted activities in compliance with the enactment on ICT system security, i.e. other enactments that regulate security of its information system.

**Maintenance of Contracted Level of Information Security and Provided Services in Compliance with Requirements Contracted with Service Provider**

Article 27

With the objective of maintaining the contracted level of information security and provided services in compliance with requirements that had been contracted with the service provider, the ICT system operator shall establish mechanisms for oversight over service provision, appoint a person in charge of monitoring the realization of service provision and control over the fulfilment of the level of information security, by applying corresponding procedures and establishing oversight.

**Prevention and Reacting to Security Incidents, which Implies Adequate Information Exchange on Security Weaknesses of ICT System, Incidents and Threats**

Article 28

The ICT operator shall be under obligation to determine procedures that define persons responsible that are in charge of prevention and reacting, plan for action in case of danger from onset of security incidents or onset of security incidents, obligation to keep records on undertaken activities, the obligation of reporting and information exchange on security weaknesses of the ICT system, incidents and threats.

The ICT operator should commit all employees and service providers to report to the responsible person referred to in paragraph 1 of this Article, without any delay, any security related weaknesses, threats and incidents in the ICT system.

The ICT operator shall be under obligation to assign a person responsible for reporting to competent authorities on incidents in the ICT system that could have a significant impact on disrupting information security.

The ICT operator should define and apply procedures that should ensure processes for identification, collecting and keeping information hat may serve as evidence for initiation of disciplinary, misdemeanour or criminal proceedings.

## Measures that Ensure Continuity of Performance of Tasks in Extraordinary Circumstances

Article 29

The ICT operator should envisage measures that ensure performance of tasks is extraordinary circumstances, and which shall imply maintenance of information security at a satisfactory level, definition of responsibilities, plans, procedures in case or extraordinary events and procedures for recovery of the ICT system, within the framework of regular procedures of maintaining information security or adoption of special procedures.

The ICT operator should establish, document, implement and maintain processes, procedures and control in order to ensure the required level of continuity of business operations during an extraordinary situation.

The ICT operator should verify established and implemented controls of business continuity in regular conditions of work, in order for them to be valid and effective during an extraordinary situation.

The ICT operator should identify requirements for accessibility of the ICT system. Redundant components should be taken under consideration when accessibility cannot be guaranteed by using existing system architecture.

## Final Provision

Article 30

This Decree shall enter into effect on the eighth day from the date of its publication in the “Official Gazette of the Republic of Serbia”.