Pursuant to Article 11, paragraph 9 of the Law on Information Security (Official Gazette of the RS, No. 6/16, 94/17 and 77/19) and Article 42, paragraph 1 of the Law on Government (Official Gazette of the RS, No. 55/05, 71/05 – corrigendum, 101/07, 65/08, 16/11, 68/12 – CC, 72/12, 7/14 – CC, 44/14 and 30/18 – other law),

The Government has passed

REGULATION

On the incident notification procedure in information and communication systems of special importance

Subject matter of the Regulation

Article 1

This Rulebook shall regulate the procedure for notification of incidents in information and communications systems of special importance (hereinafter: ICT systems of special importance) with the potential to exert significant adverse impact on information security.

The Regulation shall additionally regulate the list, the types and the significance of incidents according to the threat levels, as well as the actions and exchange of information on incidents among the authorities whose representatives are appointed members of the Coordination Body for Information Security (hereinafter: the Coordination Body).

Incident notification procedure

Article 2

Operators of ICT systems of special importance shall provide notifications of incidents in an ICT system with the potential to exert significant adverse impact on information security without delay, and on the following business day from the day on which they have learnt of the occurrence of the incident at the latest, in compliance with the law.

Notifications of incidents shall be delivered through the website of the Ministry in charge of information security (hereinafter: the Ministry) or of the National Centre for the Prevention of Security Risks in ICT Systems (hereinafter: the National CERT) into the single system for receipt of notifications of incidents (hereinafter: the single system) which shall be maintained by the Ministry.

Operators of the ICT systems of special importance that are carrying out the tasks of financial institutions and the tasks of keeping registers of information on liabilities of natural and legal persons to financial institutions shall deliver notifications of incidents to the National Bank of Serbia, without delay, on the following business day from the day on which they have learnt of the occurrence of the incident at the latest.

Operators of the ICT systems of special importance that are carrying out activities in the field of electronic communications shall deliver the notifications of incidents to the regulatory body for electronic communications (hereinafter: RATEL), without delay, on the following business day from the day on which they have learnt of the occurrence of the incident at the latest.

The National Bank of Serbia and RATEL shall deliver the notifications received referred to in paragraphs 3 and 4 of this Article into the single system, without delay, and on the following business days from the receipt of these notifications at the latest, in compliance with the law.

Authorities that, in compliance with this Regulation, act in cases of incidents in ICT systems of special importance and exchange information on such incidents shall provide protection of information on such incidents in compliance with regulations and shall use such information solely for the purpose for which it has been obtained.

Contents of a notification of incident

Article 3

A notification of incident must comprise the following information:

1) Name of the person submitting the report, telephone number and electronic mail address,

2) Type and description of the incident,

3) Date and time of the beginning of the incident and the duration of the incident,

4) Consequences of the incident,

5) Activities taken with a view to mitigating the consequences of the incident,

6) Where necessary, other pieces of relevant information.

In cases of emergencies, the notification of incident shall additionally be made by telephone, through the electronic mail or in some other appropriate manner.

The Ministry, the National Bank of Serbia and RATEL may regulate the incident notification procedure in more detail, in compliance with this Regulation.

List of Incidents according to types

Article 4

The types of incidents in the ICT systems of special importance with the potential to exert significant adverse impact on information security shall be classified in incident groups, in compliance with the List of Incidents according to incident types that is presented in Appendix 1 which is printed with this Regulation and is an integral part hereof.

Significance of incidents

Article 5

Incidents in the ICT systems of special importance with the potential to exert significant adverse impact on information security shall be classified according to the threat levels, bearing in mind the consequences of the incidents, in compliance with the Classification of Incidents according to the Threat Levels (hereinafter: the Classification) that is presented in Appendix 2 which is printed with this Regulation and is an integral part hereof.

Gathering, analysis and exchange of information on security risks for the ICT systems

Article 6

Upon receipt of a notification of incident in an ICT system of special importance, the National CERT shall act in compliance with the competences laid down by the law, i.e. it shall gather, analyse and exchange information on security risks for the ICT system, as well as on the incident, and shall notify, provide support, warn and advise the operator of the ICT system of special importance in relation to that and perform other tasks within its remit.

Upon having completed an analysis, the National CERT shall determine the incident threat level, in compliance with the Classification of Incidents according to the significance of the threat level (Appendix 2).

The National CERT shall proceed with providing warnings and advice to the public on the incidents with the potential to exert significant adverse impact on information security of the ICT systems of special importance in the Republic of Serbia upon having obtained the consent thereon from the Ministry.

Acting in cases of incidents related to the commission of criminal offences, jeopardizing defence of the Republic of Serbia or threats to national security

Article 7

The authorities referred to in Article 2 of this Regulation shall, without delay, deliver notifications of incidents to the competent authorities, in compliance with the law, if the incident is related to:

1) Commission of criminal offences which are prosecuted *ex officio*,

2) Significant compromising of information security, which has or may have as a consequence jeopardizing of defence of the Republic of Serbia,

3) Significant compromising of information security, which has or may have as a consequence jeopardizing of national security.

Acting in cases of incidents of the threat level of "Very High"

Article 8

In case of an incident which is assigned the threat level of "Very High" in compliance with the Classification, the National CERT shall without delay notify the Ministry thereof, which shall then notify the Republic Emergency Management Authority that shall act in compliance with the competencies laid down by the regulations.

In cases of incidents referred to in paragraph 1 of this Article, the Ministry shall convene a session of the Coordination Body.

During the duration of the incident, the National CERT shall regularly inform the Ministry and the Coordination Body of the activities taken, and following the end of the

incident it shall deliver a report on the outcome of the incident within three days at the latest, through the single system.

Acting in cases of incidents of the threat level of "High"

Article 9

In case of an incident which is assigned the threat level of "High" in compliance with the Classification, the National CERT shall without delay notify the Ministry thereof, which shall then convene a session of the Coordination Body.

The National CERT shall call a meeting with the representatives of the Ministry, public authorities' CERT and CERTs of independent operators for the purpose of their coordination during the response to the incident reported, in compliance with the competences.

Where necessary, representatives of special CERTs as well as other persons shall be present in the meetings referred to in paragraph 2 of this Article.

In the case that it is necessary, the cyber security inspector may prohibit the use of procedures and technical means which are presenting threats to or compromising information security in the ICT system of special importance and may leave a time limit for that, in compliance with the law.

During the duration of the incident, the National CERT shall regularly inform the Ministry and the Coordination Body of the activities taken, and following the end of the incident it shall deliver a report on the incident within three days at the latest, through the single system.

Following a completed assessment, the Ministry may inform the public of the incident, or provide consent to the National CERT for public notification.

Acting in cases of incidents of the threat level of "Medium"

Article 10

In case of an incident which is assigned the threat level of "Medium" in compliance with the Classification, the National CERT shall without delay notify the Ministry thereof, which shall then, in case that they assess that to be necessary, convene a session of the Coordination Body.

The National CERT shall prepare a proposal of recommendations for actions and contact the ICT system of special importance in which the incident has occurred, in order to implement the proposed recommendations for actions.

During the duration of the incident, the National CERT shall regularly inform the Ministry of the activities taken, and following the end of the incident it shall deliver a report on the incident within three days at the latest, through the single system.

Following a completed assessment, the Ministry may inform the public of the incident, or provide consent to the National CERT for public notification.

Acting in cases of incidents of the threat level of "Low"

Article 11

In case of an incident which is assigned the threat level of "Low" in compliance with the Classification, the National CERT shall notify the Ministry thereof.

Where necessary, the National CERT shall prepare a proposal of recommendations for actions and contact the ICT system of special importance in which the incident has occurred.

During the duration of the incident, the National CERT shall regularly inform the Ministry of the measures taken, and following the end of the incident it shall deliver a report on the incident within three days at the latest, through the single system.

Termination of previous regulation

Article 12

On the date of entry into force of this Regulation, the Regulation on procedure for delivery of information, lists, types and significance of incidents and notification procedure for incidents in information and communication systems of special importance (Official Gazette of the RS, No. 94/16) shall cease to be in force.

Final provision

Article 13

This Regulation shall enter into force on the eighth day from the date of its publication in the Official Gazette of the Republic of Serbia.

05 number 110-364/2020-1

In Belgrade, on February 6, 2020

The Government

The Prime Minister,

Ana Brnabic, own signature

Appendix 1

LIST OF INCIDENTS ACCORDING TO TYPES	
Incidents' group	**Type of incident**
Installation of malicious code ("malware" in English) within the ICT system	Virus
	Worm
	Ransomware
	Trojan
	Spyware
	Rootkit
Unauthorized gathering of information	Scanning
	Sniffing
	Social engineering (impersonation and other forms)
	Compromising or release of information ("data breaches" in English)
Fraud	Phishing
	Unauthorized use of resources ("cryptojacking" in English, and other forms)
ICT system intrusion attempts	Attempt at exploiting system vulnerabilities
	Attempt at uncovering credentials ("brute force attack", "dictionary attack", etc. in English)
ICT system intrusion	Uncovering or unauthorized use of privileged accounts ("privileged account compromise" in English)
	Uncovering or unauthorized use of unprivileged accounts ("unprivileged account compromise" in English)
	Application compromise
	A network of infected devices ("botnet" in English)
Unavailability or limited availability of an ICT system	Attack aimed at preventing or disrupting operation of an ICT system ("denial-of-service attack" – DoS in English)
	Distributed attack aimed at preventing or disrupting operation of an ICT system ("distributed denial-of-service attack" – DDoS in English)
	Sabotage
	Suspension of operation of the system or a part of the system

LIST OF INCIDENTS ACCORDING TO TYPES	
Incidents' group	**Type of incident**
	("outage" in English)
Threats to security of information	Unauthorized access to information
	Unauthorized modification or deletion of information
	Cryptographic attack
Operational incidents	Failure of hardware components
	Operational issues with software components
Incidents relating to physical and technical threats to security	Theft of hardware components
	Fire
	Flooding
Other incidents	Incidents that cannot be classified in the above listed categories

Appendix 2

CLASSIFICATION OF INCIDENTS ACCORDING TO THE THREAT LEVELS	
Threat level	**Consequences of the incident**
Very high	In case of occurrence of circumstances that include threats to, disruption of operation or prevention of operation of an ICT system of special importance, and where the risks, threats or consequences of the incident for the population, material resources or the environment are of such scope and intensity that it is not possible to prevent or eliminate their occurrence or consequences through the regular actions of the competent authorities and services, due to which it is necessary to employ special measures, additional forces and means with an intensified operational regime for their mitigation and removal.
High	Cases where the risks and threats or the consequences incurred by the incident for the population, material resources or the environment are of such scope and intensity that their occurrence or consequences can be prevented or removed through the regular actions of the competent authorities and services.
Medium	Cases where the risks, threats or the consequences incurred by the incident are of such scope and intensity that they can be removed through joint action of the ICT system of special importance in which the incident has occurred and the National CERT.
Low	Cases where the risks, threats or the consequences incurred by the incident are of such scope and intensity that they can be removed by the actions of the ICT system of special importance.