COLLECTION OF LAWS OF
THE SLOVAK REPUBLIC

2018

Declared: June 14, 2018 Time version of the regulation effective from: June 15, 2018

Content is legally binding.

166

DECREE

of the National Security Authority

of June 1, 2018,

on details on the technical, technological and personnel capabilities of the cybersecurity incidents handling unit

The National Security Authority pursuant to Section 32 Par. 1 item a) of the Act No. 69/2018 on Cybersecurity and on the Amendment to Certain Acts (hereinafter referred to as "the Act") stipulates:

Article 1

This Decree establishes the details of the technical, technological and personnel capabilities of the unit for cybersecurity incidents handling (hereinafter referred to as the "CSIRT unit", the details and manner of compliance of which are demonstrated for the purpose of accrediting the CSIRT pursuant to Section 13 of the Act.

Article 2

(1) The required equipment of the CSIRT unit pursuant to Section 14 item a) of the Act is proved by fulfilment

a) technical conditions, including technical and organisational conditions and technical process conditions,

b) personnel conditions and

c) technological conditions.

(2) The fulfilment of the conditions under Paragraph 1 is documented in such a way that every worker of the CSIRT unit who performs the tasks of this CSIRT unit has access to it and is demonstrably familiar with it in the form of a binding internal regulation issued by a public authority pursuant to Section 4 item b) of the Act.

(3) The document under Paragraph 2 is part of the documentation demonstrating compliance with the CSIRT unit accreditation conditions under Section 14 of the Act.

Article 3

(1) Technical conditions that include technical and organisational conditions include

a) specifying the mandate of the CSIRT unit,

b) defining entities within the sector and sub-sector according to Annex 1 of the Act that use or are connected to CSIRT unit services (hereinafter referred to as the "Customer"),

c) defining the powers of the CSIRT unit,

d) defining the CSIRT unit tasks,

e) defining the services provided by the CSIRT unit,

f) defining the reaction time of services provided by the CSIRT unit,

g) the classification of cybersecurity incidents addressed by the CSIRT unit,

h) defining the organisational structure of the CSIRT unit,

i) defining the CSIRT unit security policy.

(2) The technical and organisational condition referred to in Paragraph 1 item a) determines the establishment and operation of a CSIRT unit pursuant to Section 9 Par. 2 of the Act.

(3) The technical and organisational condition pursuant to Paragraph 1 item b) means that the CSIRT unit has a clearly defined customer structure to which it provides its services.

(4) The technical and organisational condition pursuant to Paragraph 1 item c) means that the CSIRT unit has defined rights that it is entitled to perform in relation to its customer structure.

(5) The technical and organisational condition pursuant to Paragraph 1 item d) means that the CSIRT unit performs its tasks in accordance with Section 15 of the Act.

(6) The technical and organisational condition pursuant to Paragraph 1 item e) means that the CSIRT unit has defined services pursuant to Section 15 Par. 2 and 3 of the Act that provides its customer structure.

(7) The technical and organisational condition pursuant to Paragraph 1 item f) means that the CSIRT unit has a specified response time for the received information as the time of receiving the cyber-relevant information
(incidents, threats or vulnerabilities) during the first actions of CSIRT unit. In responding to a cybersecurity incident, the maximum reaction time is two working days after receiving the cyber-relevant information.

(8) The technical and organisational condition pursuant to Paragraph 1 item g) means that the CSIRT unit has a created scheme for the classification and sorting of cybersecurity incidents into individual categories according to a separate regulation.[1)]

(9) The technical and organisational condition referred to in Paragraph 1 item h) means that the CSIRT unit has a designated organisational structure that defines the different workplaces and roles and has a defined relationship and position of the CSIRT unit within the Competent Body or in relation to the Competent Body to perform the tasks of the CSIRT unit.

(10) The technical and organisational condition pursuant to Paragraph 1 item i) means that the CSIRT unit has a security policy that is based on the generally binding legal regulations of the Slovak Republic and international security standards. Security policy means a set of security requirements for security at all affected levels of the CSIRT unit organisation.

Article 4

(1) Technical conditions that include technical process conditions are defining

a) escalation processes to the level of management,

b) escalation processes at the level of media communication,

c) the cybersecurity incident prevention process,

d) the process of detecting cybersecurity incidents,

e) cybersecurity incident handling process,

f) incident handling process that is not a cybersecurity incident under Section 3 item j) of the Act, but by their nature they may interfere with the security of the network or the information system,

g) the audit and control process of the CSIRT unit,

h) the availability of emergency services,

i) the process of dealing with e-mail accounts and websites,

j) the process of safe dealing with information,

k) the process of obtaining and dealing with information resources,

l) process of active help to the customer structure,

m) process of communication with the Competent Body performing the tasks of the CSIRT unit,

n) the process of creating and sharing statistics,

o) the internal meetings of the CSIRT unit,

p) cooperation with partner organisations.

(2) Technical and procedural condition referred to in Paragraph 1 item a) means that the CSIRT unit has defined escalation processes at the level of the CSIRT unit management, the level of management of the Competent Body to perform the tasks of the CSIRT unit and the level of the national CSIRT unit.

(3) Technical and procedural condition referred to in Paragraph 1 item b) means that the CSIRT unit has defined escalation processes for the media communication needs of the information received in the CSIRT unit activity.

(4) Technical and procedural condition referred to in Paragraph 1 item c) means that the CSIRT unit has defined procedures in which it prevents cybersecurity incidents within its customer structure, in particular by building security awareness.

(5) Technical and procedural condition referred to in Paragraph 1 item d) means that the CSIRT unit has defined procedures in which it detects and evaluates cybersecurity incidents within its customer structure.

(6) Technical and procedural condition referred to in Paragraph 1 item e) means that the CSIRT unit has defined procedures in which it responds to cybersecurity incidents and handles cybersecurity incidents within its customer structure.

(7) Technical and procedural condition referred to in Paragraph 1 item f) means that the CSIRT unit has a defined procedure in which it responds to cybersecurity incidents within its customer structure and addresses cybersecurity incidents that cannot be handled by standard procedures.

(8) Technical and procedural condition referred to in Paragraph 1 item g) means that the CSIRT unit has a defined procedure for setting control mechanisms within the CSIRT unit, and how and how often checks are performed.

(9) Technical and procedural condition referred to in Paragraph 1 item h) means that the CSIRT unit has a defined procedure to respond to cybersecurity incidents or cybernetic relevant emergency information, even at off-time.

(10) Technical and procedural condition referred to in Paragraph 1 item i) means that the CSIRT unit has a defined procedure such as how e-mail accounts are created, how they are dealing with, and who has access to those e-mail accounts, what information is available on the CSIRT unit website, how the website is changed and updated.

(11) Technical and procedural condition referred to in Paragraph 1 item j) means that the CSIRT unit has defined procedures for classifying, protecting, storing and disposing of information and managing access to it.

(12) Technical and procedural condition referred to in Paragraph 1 item k) means that the CSIRT unit has a defined procedure by which it acquires and verifies the information sources.

(13) Technical and procedural condition referred to in Paragraph 1 item l) means that the CSIRT unit has a communication process with its customer structure and shares information with it.

(14) Technical and procedural condition referred to in Paragraph 1 item m) means that the CSIRT unit has a defined communication procedure with the Competent Body and how it communicates to it the information about its activities.

(15) Technical and procedural condition referred to in Paragraph 1 item n) means that the CSIRT unit has a defined procedure by which it creates and shares the statistics generated by its activity.

(16) Technical and procedural condition referred to in Paragraph 1 item o) means that the CSIRT unit has a defined procedure, how often and at what level the CSIRT unit staff meetings are organised.

(17) Technical and procedural condition referred to in Paragraph 1 item p) means that the CSIRT unit has a defined procedure, how often and at what level it communicates and shares information with its partner organisations and other CSIRT units.

Article 5

(1) Personnel conditions include

a) the Code of Conduct and the Practical Performance Code in the CSIRT unit,

b) availability of CSIRT unit staff,

c) qualification prerequisites for CSIRT unit staff,

d) internal training rules for CSIRT unit staff,

e) external technical training rules for CSIRT unit staff,

f) rules for external communication training for CSIRT unit staff,

g) rules for external meetings of CSIRT unit staff.

(2) Personnel condition under Paragraph 1 item a) means that a CSIRT unit is issued with the Code of Conduct and the Practical Performance Code in the CSIRT unit or other comparable document that contains the principles of work and behaviour.

(3) Personnel condition under Paragraph 1 item b) means that the CSIRT unit has a minimum of at least three workers who are responsible for fulfilling the tasks of the CSIRT unit.

(4) Personnel condition under Paragraph 1 item c) means that the CSIRT unit has a framework of qualification prerequisites for staff who perform the tasks of the CSIRT unit and which includes

a) proof of English language knowledge at least at B1 level of the Common European Framework of Reference for Languages by at least one worker of the CSIRT unit and

b) demonstration of information technology education by at least two workers of the CSIRT unit within the scope of a special regulation.

(5) Personnel condition under Paragraph 1 item d) means that the CSIRT unit has a program of in-house training for staff, indicating their specialisation and regularity.

(6) Personnel conditions under Paragraph 1 item e) and f) mean that the CSIRT unit has a program for external technical and external communication training, together with their specialisation and regularity.

(7) Personnel condition under Paragraph 1 item g) means that the CSIRT unit has defined opportunities to participate in external meetings of CSIRT units within existing CSIRT unit communities and groups.

Article 6

(1) Technological conditions include

a) the method of collecting data about customers´ assets and a list of customers´ assets,

b) a list of information sources

c) a consolidated e-mail system,

d) incident monitoring system,

e) availability of telephone services,

f) availability of e-mail services,

g) availability of Internet access,

h) tools to prevent incidents.

(2) Technological condition under Paragraph 1 item a) means that the CSIRT unit has a defined manner and periodicity for collecting data on customer assets and records of those assets. Data collection and list of assets serve to address alerts and warnings, and to inform customers more effectively about specific cybernetic relevant information.

(3) Technological condition under Paragraph 1 item b) means that the CSIRT unit has a created and maintained list of information sources from which it draws cybernetic relevant information that may affect cybersecurity.

(4) Technological condition under Paragraph 1 item c) means that the CSIRT unit has a secure e-mail system that allows the CSIRT unit workers to access all of the e-mail accounts of the CSIRT unit that are required to fulfil the tasks of the CSIRT unit.

(5) Technological condition under Paragraph 1 item d) means that the CSIRT unit has a system that enables the incident to be recorded and handled within the cybersecurity incident handling, make changes and maintain all the necessary information about the incident.

(6) Technological condition under Paragraph 1 item e) means that the CSIRT unit has a redundant connection to the telecommunication network to ensure continuity of CSIRT unit tasks.

(7) Technological conditions referred to in Paragraph 1 item f) and g) mean that the CSIRT unit has a redundant Internet connection to ensure continuity of CSIRT unit tasks.

(8) Technological condition under Paragraph 1 item h) means that the CSIRT unit has systems that are technologically used to prevent cybersecurity incidents

Article 7

(1) Technical, technological and personnel capabilities of a CSIRT unit cannot be demonstrated by complying with other or substitute terms and conditions that are not listed in this Decree.

(2) Request for CSIRT unit compliance assessment with CSIRT unit accreditation conditions under Section 13 Par. 1 of the Act contains

a) designation of a public authority pursuant to Section 4 item b) of the Act,

b) name and surname of the person responsible for the correctness of the application,

c) documentation or change in documentation,

d) date and signature of applicant.

Article 8

This Decree adopts the legally binding acts of the European Union stated in the Annex.

Article 9

This Decree enters into force on June 15, 2018.

Jozef Magala

1) Section 2 Par. 2 of the Decree of the National Security Authority No. 165/2018 which specifies the identification criteria for each category of serious cybersecurity incident and the details of reporting cybersecurity incidents.

Annex
to the Decree No. 166/2018

LIST OF ADOPTED LEGALLY BINDING ACTS OF THE EUROPEAN UNION

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high common level of network and information systems in the Union (OJ L 194, 19 July 2016).

Publisher of the Laws of the Slovak Republic, the content administrator and the operator of the legal and information portal Slov-Lex available at website of www.slov-lex.skje
the Slovak Republic´s Ministry of Justice, Župné námestie 13, 813 11 Bratislava, tel.: 02 888 91 137, fax: 02/52442853, e-mail: helpdesk@slov-lex.sk.