THE ACT ON CYBER SECURITY

according to the legal state of August 1, 2017

The obligations of authorities and legal or natural persons according Act No 181/2014 Coll. on Cyber Security

National Cyber and Information Security Agency

Electronic communications service means a service usually provided for payment which is based on the transmission of signals through electronic communication networks, including telecommunication services and transmission services in networks used for radio and television broadcasting and networks for cable distribution, with exception of services that offer content through networks and services of electronic communications or perform editorial control over the content transmitted by networks and provided services of electronic communications; it does not include the services of information society which do not completely or mostly lie in the transmission of signals through electronic communications.
(Section 2, letter n) of Act No 127/2005 Coll. on Electronic Communication and on the Change of Some Related Acts (Electronic Communications Act))

Electronic communication network means a transmission systems or a coupling or a routing device or other devices, including network elements that are not active, which allow the transmission of signals through lines, radio, optical or other electromagnetic means, including satellite networks, wired networks with the commutation of circuits or packets and land mobile networks, electricity cable systems within reach in which they are used for the transmission of signals, networks for radio and television broadcasting and networks for cable distribution, regardless of the type of transmitted information.
(Section 2, letter h) of Act No 127/2005 Coll. on Electronic Communication and on the Change of Some Related Acts (Electronic Communications Act))

Important network means an electronic communication network providing direct international connectivity to public communication networks or providing direct connection to a critical information infrastructure
(Section 2, letter h) of Act No 181/2014 Coll. on Cyber Security)

Digital service means a service of information society according to the Act on Certain Information Society Services that consists of the provision of an online marketplace, a search engine or cloud computing
(Section 2, letter l) of Act No 181/2014 Coll. on Cyber Security)

Critical information infrastructure means an element or system of elements of the critical infrastructure in the sector of communication and information systems within the field of cyber security
(Section 2, letter b) of Act No 181/2014 Coll. on Cyber Security)

Important information system means an information system operated by a public authority that execute public powers that is neither a critical information infrastructure nor an information system of essential service, and which may endanger or noticeably limit the execution of public powers in the case of an information security breach
(Section 2, letter d) of Act No 181/2014 Coll. on Cyber Security)

Information system of essential service means an information system on which the provision of an essential service is dependent
(Section 2, letter f) of Act No 181/2014 Coll. on Cyber Security)

Essential service means a service the provision of which is dependent on electronic communication networks or information systems, and the disruption of which may have a significant impact on the security of societal or economic activities in any of the following sectors: Energy, Transport, Banking, Financial market infrastructures, Health sector, Water resource management, Digital infrastructure and Chemical industry
(Section 2, letter i) of Act No 181/2014 Coll. on Cyber Security)

version 1.0, March 2018

Note: The national CERT is operated by CSIRT.CZ which is managed by CZ.NIC .

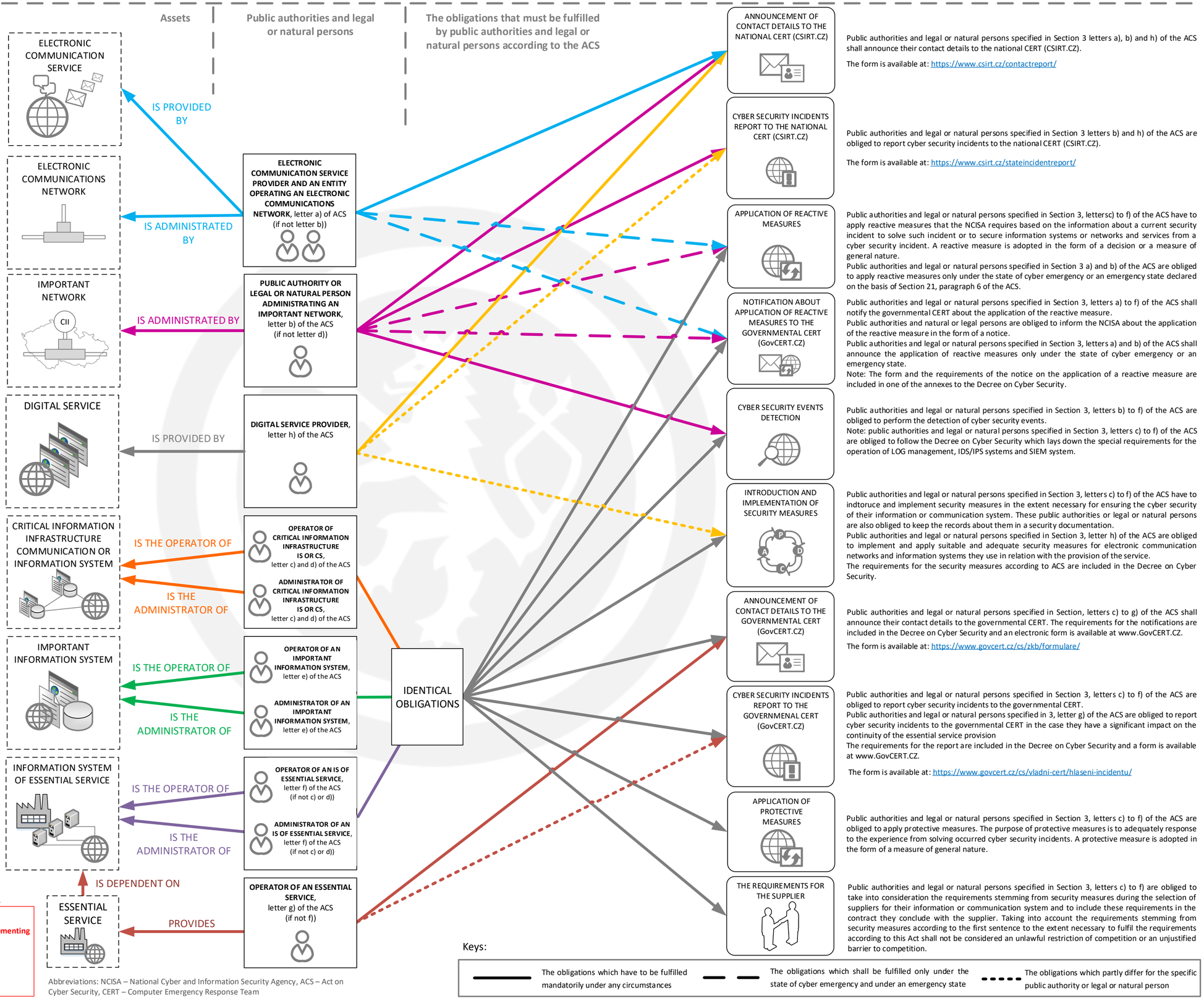
Note:

This document is only a supporting guide and does not replace any act or implementing legislation.

This document does not include an exhaustive summary of all rights and obligations.

The right to make changes to this document reserved.

This document is non-binding English translation.



Public authorities and legal or natural persons specified in Section 3 letters a), b) and h) of the ACS shall announce their contact details to the national CERT (CSIRT.CZ).

The form is available at: https://www.csirt.cz/contactreport/

Public authorities and legal or natural persons specified in Section 3 letters b) and h) of the ACS are obliged to report cyber security incidents to the national CERT (CSIRT.CZ).

The form is available at: https://www.csirt.cz/stateincidentreport/

Public authorities and legal or natural persons specified in Section 3, lettersc) to f) of the ACS have to apply reactive measures that the NCISA requires based on the information about a current security incident to solve such incident or to secure information systems or networks and services from a cyber security incident. A reactive measure is adopted in the form of a decision or a measure of general nature.
Public authorities and legal or natural persons specified in Section 3 a) and b) of the ACS are obliged to apply reactive measures only under the state of cyber emergency or an emergency state declared on the basis of Section 21, paragraph 6 of the ACS.

Public authorities and legal or natural persons specified in Section 3, letters a) to f) of the ACS shall notify the governmental CERT about the application of the reactive measure.
Public authorities and natural or legal persons are obliged to inform the NCISA about the application of the reactive measure in the form of a notice.
Public authorities and legal or natural persons specified in Section 3, letters a) and b) of the ACS shall announce the application of reactive measures only under the state of cyber emergency or an emergency state.
Note: The form and the requirements of the notice on the application of a reactive measure are included in one of the annexes to the Decree on Cyber Security.

Public authorities and legal or natural persons specified in Section 3, letters b) to f) of the ACS are obliged to perform the detection of cyber security events.
Note: public authorities and legal or natural persons specified in Section 3, letters c) to f) of the ACS are obliged to follow the Decree on Cyber Security which lays down the special requirements for the operation of LOG management, IDS/IPS systems and SIEM system.

Public authorities and legal or natural persons specified in Section 3, letters c) to f) of the ACS have to indtoruce and implement security measures in the extent necessary for ensuring the cyber security of their information or communication system. These public authorities or legal or natural persons are also obliged to keep the records about them in a security documentation.
Public authorities and legal or natural persons specified in Section 3, letter h) of the ACS are obliged to implement and apply suitable and adequate security measures for electronic communication networks and information systems they use in relation with the provision of the service.
The requirements for the security measures according to ACS are included in the Decree on Cyber Security.

Public authorities and legal or natural persons specified in Section, letters c) to g) of the ACS shall announce their contact details to the governmental CERT. The requirements for the notifications are included in the Decree on Cyber Security and an electronic form is available at www.GovCERT.CZ.

The form is available at: https://www.govcert.cz/cs/zkb/formulare/

Public authorities and legal or natural persons specified in Section 3, letters c) to f) of the ACS are obliged to report cyber security incidents to the governmental CERT.
Public authorities and legal or natural persons specified in 3, letter g) of the ACS are obliged to report cyber security incidents to the governmental CERT in the case they have a significant impact on the continuity of the essential service provision
The requirements for the report are included in the Decree on Cyber Security and a form is available at www.GovCERT.CZ.

The form is available at: https://www.govcert.cz/cs/vladni-cert/hlaseni-incidentu/

Public authorities and legal or natural persons specified in Section 3, letters c) to f) of the ACS are obliged to apply protective measures. The purpose of protective measures is to adequately response to the experience from solving occurred cyber security incidents. A protective measure is adopted in the form of a measure of general nature.

Public authorities and legal or natural persons specified in Section 3, letters c) to f) are obliged to take into consideration the requirements stemming from security measures during the selection of suppliers for their information or communication system and to include these requirements in the contract they conclude with the supplier. Taking into account the requirements stemming from security measures according to the first sentence to the extent necessary to fulfil the requirements according to this Act shall not be considered an unlawful restriction of competition or an unjustified barrier to competition.

Keys:

- The obligations which have to be fulfilled mandatorily under any circumstances
- The obligations which shall be fulfilled only under the state of cyber emergency and under an emergency state
- The obligations which partly differ for the specific public authority or legal or natural person

Abbreviations: NCISA – National Cyber and Information Security Agency, ACS – Act on Cyber Security, CERT – Computer Emergency Response Team