Ordinance on Protection against Cyber Risks in the Federal Administration

(Cyber Risks Ordinance, CyRV)

of 27 May 2020 (Status as of 1 April 2021)

The Swiss Federal Council,

on the basis of Article 30 of the Federal Act of 21 March 1997[1] on Measures to Safeguard Internal Security
and on Articles 43 paragraphs 2 and 3, 47 paragraph 2 and 55 of the Government and Administration Organisation Act of 21 March 1997[2],

ordains:

Chapter 1 General Provisions

Art. 1 Subject matter

This Ordinance regulates the organisation of the Federal Administration for its protection against cyber risks as well as the tasks and responsibilities of the various offices in the cyber security domain.

Art. 2 Scope of application

This Ordinance applies to:

a. the administrative units of the central Federal Administration in accordance with Article 7 the Government and Administration Ordinance of 25 November 1998[3];

b.[4] the offices that undertake in accordance with Article 2 paragraph 2 of the Ordinance of 25 November 2020[5] on the Digital Transformation and ICT (DTIO) to comply therewith.

AS **2020** 2107

1 SR **120**
2 SR **172.010**
3 SR **172.010.1**
4 Amended by Annex No 1 of the O of 25 Nov. 2020 on the Digital Transformation and ICT, in force since 1 Jan. 2021 (AS **2020** 5871).
5 SR **172.010.58**

Art. 3 Definitions

In this Ordinance:

a. *cyber security* means the desired state in which data processing via information and communication infrastructures, in particular the exchange of data between persons and organisations, works as intended;

b. *cyber incident* means an unintended or intended but unauthorised event that leads to the confidentiality, integrity, availability or comprehensibility of data being adversely affected or that may lead to malfunctions;

c. *cyber risk* means the risk of a cyber incident, the extent of which is measured by the product of the probability of occurrence and the extent of the damage potentially caused;

d. *resilience* means the ability of a system, organisation or society to withstand internal or external disruptions and to maintain proper functionality or restore it as quickly and completely as possible;

e. *information technology security* means the aspect of cyber security that relates to technical systems;

f. *IT security directives* means the security standards that apply to the organisational measures, processes, services and technology;

g. *critical infrastructures* means processes, systems and facilities that are essential for the proper functioning of the economy or the well-being of the population;

h.[6] *protected IT systems* is a generic term for applications, services, systems, networks, data collections, infrastructures and information technology products; protected IT systems can include a combination of several identical or related systems;

Chapter 2 Principles governing Protection against Cyber Risks

Art. 4 Goals

[1] The Federal Administration shall ensure that its organs and systems are suitably resilient to cyber risks.

[2] It shall work with the cantons, the communes, the private sector, society, academia and international partners provided this serves to protect its own security interests, and shall encourage the exchange of information.

6 Inserted by No I of the O of 24 Feb. 2021, in force since 1 April 2021 (AS **2021** 132).

Art. 5 National strategy for the protection of Switzerland against cyber risks

The Federal Council shall set out in a national strategy for the protection of Switzerland against cyber risks (NCS) the strategic framework for improving the prevention and early detection of and the reaction and resilience to cyber risks.

Art. 6 Domains

The measures to protect against cyber risks are divided into the following three domains:

a. cyber security domain: all measures that serve to prevent and manage incidents and to improve resilience against cyber risks and that strengthen international cooperation for this purpose;

b. cyber defence domain: all intelligence and military measures designed to protect critical systems, defend against attacks in cyberspace, ensure the operational readiness of the Armed Forces in all situations, and build capacities and capabilities to provide subsidiary support to civilian authorities; they include active measures to recognise threats, to identify aggressors and to disrupt and stop attacks;

c. cyber prosecution domain: all measures taken by the police and federal and cantonal prosecutors to combat cyber crime.

Chapter 3 Organisation and Responsibilities

Section 1 Cross-Departmental Cooperation

Art. 7 Federal Council

The Federal Council shall carry out the following tasks:

a. It monitors the implementation of the NCS on the basis of the strategic controlling and decides on measures as required.

b. It shall within the scope of its responsibilities specify the areas in which directives on protection against cyber risks are required or must be revised.

c. It shall issue directives on protecting the Federal Administration against cyber risks.

d. It shall authorise derogations from its directives.

Art. 8 Cyber Core Group

[1] The Cyber Core Group (CyCG) shall comprise:

a. the Federal Cyber Security Delegate (Art. 6*a* of the Federal Department of Finance Organisation Ordinance of 17 Feb. 2010[7]) as the representative of the Federal Department of Finance (FDF);

b. a representative of the Federal Department of Defence, Civil Protection and Sport (DDPS);

c. a representative of the Federal Department of Justice and Police (FDJP);

d. a representative of the cantons appointed by the Conference of Cantonal Governments.

2 The Federal Cyber Security Delegate chairs the Group.

3 The CyCG shall inform representatives of other federal administrative units that are active in connection with cyber risks about its agenda and may invite them to attend individual meetings. Where matters have a foreign policy dimension, it may involve the Federal Department of Foreign Affairs (FDFA). In addition it may involve experts from the private sector and the universities.

4 The CyCG has the following tasks in particular:

a. It assesses current cyber risks and their potential development on the basis of information from the domains of cyber security, cyber defence and cyber prosecution.

b. It continuously evaluates the existing systems in the domains of cyber security, cyber defence and cyber prosecution and checks whether these are adapted to the threat situation.

c. It provides support, if necessary with other offices, for interdepartmental incident management.

d. It informs the Federal Security Core Group (SCG) about cyber incidents and developments that are relevant to foreign and security-policy.

5 The three departments represented in the CyCG shall make information available for the joint assessment of a situation.

6 The Federal Intelligence Service is responsible for presenting the overall cyber threat situation to the CyCG.

Art. 9 Steering Committee for the National Strategy for the Protection of Switzerland against Cyber Risks

1 The Federal Council shall appoint a Steering Committee for the National Strategy for the Protection of Switzerland against Cyber Risks (NCS StC).

2 The NCS StC shall comprise the Federal Cyber Security Delegate, representatives from the cantons appointed by the Conference of Cantonal Governments, representatives of business and the universities and representatives of the administrative units that are responsible for implementing any NCS measures in accordance with the

7 SR **172.215.1**

NCS implementation plan. Each department and the Federal Chancellery shall appoint at least one representative to the NCS StC.

3 The Federal Cyber Security Delegate chairs the Steering Committee.

4 The NCS StC has the following tasks:

a. It ensures the strategic coherence of the implementation of NCS measures and checks their progress continuously by a process of strategic controlling.

b. It draws up proposals for special measures in the event of the delayed or incomplete implementation of NCS measures.

c. It ensures the ongoing further development of the NCS; to do so it monitors the development of the threat situation in consultation with the CyCG and devises proposals for the adjustment of the NCS as required.

d. It prepares a report each year on the implementation of the NCS for the Federal Council and the public.

e. It ensures all the offices concerned from the Confederation, cantons, business and universities take a coordinated approach to implementing the NCS measures.

f. It ensures that in implementing the NCS measures account is taken of the risk policy of the Confederation, the national strategy to protect critical infrastructures and the Federal Council strategies in relation to information technology.

Art. 10 IT Security Committee

1 The IT Security Committee (ITSC) comprises a representative of the National Cyber Security Centre (NCSC[8]), the departmental and the Federal Chancellery IT security officers and the IT security officers for standard information and communication technology services (ICT).

2 Additional persons may be included in an advisory capacity on a case-by-case basis.

3 The NCSC representative chairs the committee.

4 The ITSC acts as a consultative body for the NCSC on IT security issues in the Federal Administration.

Art. 11 The Cyber Security Delegate

1 The Federal Cyber Security Delegate has the following tasks:

a. He or she chairs the NCSC.

b. He or she ensures the best possible coordination of cross-departmental work in the domains of cyber security, cyber defence and cyber prosecution.

8 Footnote not relevant to English text