

*English is not an official language of the Swiss Confederation. This translation is provided for information purposes only and has no legal force.*

## **Ordinance on the Protection of Federal Information (Information Protection Ordinance, IPO)**

of 4 July 2007 (Status as of 1 January 2021)

---

*The Swiss Federal Council,*

on the basis of Articles 8 paragraph 1 and 43 paragraph 2 of the Government and Administration Organisation Act of 21 March 1997<sup>1</sup>

and Article 150 paragraph 3 of the Armed Forces Act of 3 February 1995<sup>2</sup>,

*ordains:*

### **Section 1    General Remarks**

**Art. 1**            Subject matter

<sup>1</sup> This Ordinance regulates the protection of federal and armed forces information to the extent that national interests so require. In particular, it defines its classification and treatment.

<sup>2</sup> The specific provisions of other legislation are reserved.

**Art. 2**            Scope

This Ordinance applies:

- a. to the Federal Administration in terms of Article 6 of the Government and the Federal Administration Organisation Ordinance of 25 November 1998<sup>3</sup>;
- b. to military personnel;
- c. to the extent stipulated by federal law or accordingly agreed, to organisations and persons under public and private law who process classified information;
- d. to federal and cantonal courts that process classified information, to the extent stipulated by federal law.

AS 2007 3401

<sup>1</sup> SR 172.010

<sup>2</sup> SR 510.10

<sup>3</sup> SR 172.010.1

**Art. 3** Definitions

In this Ordinance:

- a. information means recordings on information carriers and oral statements;
- b. information carriers means information media of any kind, such as documents and carriers of text, picture, sound or other data; intermediary data such as drafts are also regarded as information carriers;
- c. processing means any activity involving information, regardless of the means used and procedures applied, in particular the compilation, use, processing, copying, making accessible, disclosing, transmitting, taking note of, conservation, archiving and destruction;
- d. author means a person, administrative unit, command authority or contractor who produces classified information;
- e. holder of classified information, confidant means a person who has been entrusted with classified information;
- f. classification means assessing certain information according to the list of classification criteria (Art. 8) and formally marking with a classification label;
- g. declassification means the cancellation of the classification label for information that is no longer sensitive;
- h. IT and telecommunication systems means systems and their integrated applications and databases;
- i. IT security means IT security safeguards confidentiality, availability, integrity and reproducibility in electronic data processing;
- j. codification means the use of designations and codenames;
- k. Encryption means state-of-the-art technical transformation of plain text.

**Section 2** Classifications**Art. 4** Classification levels

<sup>1</sup> Any person who compiles or issues information requiring protection (sensitive information) shall allocate it to one of the following levels of classification according to its degree of sensitivity:

- a. SECRET;
- b. CONFIDENTIAL;
- c. INTERNAL.

<sup>2</sup> If information carriers are physically merged to form a collection, consideration must be given as to whether it must be classified or given a higher level of classification.

**Art. 5** «SECRET» information

<sup>1</sup> Information is classified as «SECRET» if its disclosure to unauthorised persons may seriously harm national interests. The foregoing applies in particular to information, the disclosure of which may seriously compromise;

- a. the capacity to act of the Federal Assembly or Federal Council;
- b. the security of the population;
- c. the national economic supply or the security of nationally important management facilities and infrastructure;
- d. fulfilment of the duties of the Federal Administration, the Armed Forces or essential parts thereof;
- e. Switzerland's foreign policy interests or international relations;
- f. the protection of sources or individuals or the secrecy of operational resources and methods of the intelligence services.

<sup>2</sup> Carriers of information classified as «SECRET» must be numbered.

**Art. 6** «CONFIDENTIAL» information

<sup>1</sup> Information is classified as «CONFIDENTIAL» if its disclosure to unauthorised persons may harm national interests. The foregoing applies in particular to information, the disclosure of which may compromise:

- a. the free formation of opinions and decision-making of the Federal Assembly or the Federal Council;
- b. the proper implementation of specific measures by the authorities;
- c. the security of the population;
- d. national economic supply or the security of important infrastructure;
- e. fulfilment of the duties of parts of the Federal Administration or of the Armed Forces;
- f. Switzerland's foreign policy interests or international relations;
- g. relations between Confederation and the cantons or among the cantons themselves;
- h. Switzerland's economic, monetary and currency policy interests.

<sup>2</sup> Carriers of information classified as «CONFIDENTIAL» may be numbered.

**Art. 7** «INTERNAL» information

<sup>1</sup> Information is classified as «INTERNAL»:

- a. if its disclosure to unauthorised persons may be disadvantageous to national interests; and

- b. if it need neither be classified as «SECRET» nor «CONFIDENTIAL».<sup>4</sup>

<sup>2</sup> Information from abroad that is classified as «RESTRICTED» or equivalent shall be processed as «INTERNAL» information.

**Art. 8<sup>5</sup>** List of classification criteria

The General Secretaries Conference shall lay down in a list of classification criteria how certain sensitive federal data that occurs frequently must be classified.

**Art. 9** Classification subject to a time limit

Classification must be made subject to a time limit if it can be predicted when it will no longer be sensitive.

**Section 3 Holders of Classified Information**

**Art. 10** Requirements

<sup>1</sup> Persons who due to their range of duties are to be granted access to classified information must be:

- a. carefully selected;
- b. obliged to observe secrecy; and
- c. correspondingly trained and specialised.

<sup>2</sup> Whether holders of classified information that are to be granted access to «SECRET» or «CONFIDENTIAL» information must undergo a personnel security screening procedure, is governed by the Ordinance of 19. December 2001<sup>6</sup> on Personnel Security Screening.

**Art. 11** Basic and continuing education and training

The specialist knowledge of holders of classified information pertaining to information protection and IT security must be guaranteed and periodically updated.

**Art. 12** Responsibility

<sup>1</sup> Any person who processes classified information is responsible for complying with the regulations on information protection.

<sup>2</sup> Superiors shall regularly check compliance with these regulations.

<sup>4</sup> Amended by No I of the Ordinance of 30 June 2010, in force since 1 Aug. 2010 (AS 2010 3207).

<sup>5</sup> Amended by No I of the Ordinance of 30 June 2010, in force since 1 Aug. 2010 (AS 2010 3207).

<sup>6</sup> SR 120.4

## Section 4 Processing Classified Information

### Art. 13 Principles

<sup>1</sup> Compiling, disclosing and making accessible of classified information must be kept to a minimum; in doing so, the situation, assignment, purpose and time should be taken into account.

<sup>2</sup> Classified information may only be disclosed or made accessible to those persons who must know about it.

<sup>3</sup> In the case of requests for access to official documents, the relevant authority shall check whether access should be granted, restricted, postponed or refused in accordance with the Federal Act of 17 December 2004<sup>7</sup> on Freedom of Information in the Administration, regardless of any classification.

<sup>4</sup> Processing of information from abroad is governed by the relevant information protection agreement. If such an agreement does not exist, the information is processed according to the Swiss classification level that is equivalent to its classification level abroad.

### Art. 14 Evaluation of protection requirement and recipients

The author of «SECRET» information or «CONFIDENTIAL» information that is numbered shall check its sensitivity and its recipients every five years at least and always with due regard to the obligation to offer to the Federal Archives.

### Art. 15 Protection in the case of incorrect or missing classification

<sup>1</sup> Any person who suspects or establishes that information has obviously been incorrectly or mistakenly not classified must ensure its protection until its classification has been changed.

<sup>2</sup> He or she shall immediately inform the author, who shall immediately take the necessary measures.

### Art. 16 Reporting in the event of loss, abuse or risk

<sup>1</sup> Any person who discovers that classified information is at risk, has been lost or misused shall take protective measures and inform without delay his or her superior, the author and the relevant security bodies.

<sup>2</sup> In agreement with the security bodies, the author shall immediately take the necessary measures.

### Art. 17 Archiving

Classified information is archived according to the legislation on archiving.

<sup>7</sup> SR 152.3