Ordinance on the Protection of Federal Information

(Information Protection Ordinance, IPO)

of 4 July 2007 (Status as of 1 January 2018)

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[1]
and Article 150 paragraph 3 of the Armed Forces Act of 3 February 1995[2],

ordains:

Section 1 General Remarks

Art. 1 Subject matter

[1] 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.

[2] 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[3];

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

1 SR **172.010**
2 SR **510.10**
3 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

1 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.

2 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

[1] 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.

[2] Carriers of information classified as «SECRET» must be numbered.

Art. 6 «CONFIDENTIAL» information

[1] 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.

[2] Carriers of information classified as «CONFIDENTIAL» may be numbered.

Art. 7 «INTERNAL» information

[1] 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».[4]

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

Art. 8[5] 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

1 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.

2 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[6] 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

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

2 Superiors shall regularly check compliance with these regulations.

4 Amended by No I of the Ordinance of 30 June 2010, in force since 1 Aug. 2010 (AS **2010** 3207).
5 Amended by No I of the Ordinance of 30 June 2010, in force since 1 Aug. 2010 (AS **2010** 3207).
6 SR **120.4**

Section 4 Processing Classified Information

Art. 13 Principles

[1] 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.

[2] Classified information may only be disclosed or made accessible to those persons who must know about it.

[3] 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[7] on Freedom of Information in the Administration, regardless of any classification.

[4] 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

[1] 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.

[2] 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

[1] 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.

[2] 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.

7 SR **152.3**

Art. 18 Processing regulations

[1] The processing of classified information and the handling of related information carriers is regulated in the Annex.

[2] The General Secretaries Conference issues regulations on processing.[8]

[3] It regulates simplified handling of information by the intelligence services and the police according to their requirements; in doing so, it shall preserve adequate protection of information in accordance with this Ordinance.[9]

[4] The processing of information classified as «SECRET» in the joint reporting procedure under Article 15 of the Government and Administration Organisation Act of 21 March 1997 is regulated by the Federal Chancellery; in doing so, it shall provide adequate information protection in accordance with this Ordinance.[10]

Section 5 Security Bodies

Art. 19 Information protection delegate

[1] The Departments and the Federal Chancellery shall each appoint an information protection delegate.

[2] The information protection delegates have the following tasks in particular:

a. They ensure compliance with information protection in their area of responsibility.

b. They periodically check the presence and completeness of information carriers that are classified as SECRET.

Art. 20[11] Coordination Committee for Federal Information Protection

[1] The information protection delegates of the Departments and the Federal Chancellery form the Coordination Committee for Federal Information Protection (Coordination Committee).

[2] The Coordination Committee has the following tasks:

a. It prepares for the General Secretaries Conference a list of classification criteria, handling regulations and regulations for simplified handling of information by the intelligence services and the police.

b. It ensures a uniform information protection practice within the Confederation.

8 Amended by No I of the Ordinance of 30 June 2010, in force since 1 Aug. 2010 (AS **2010** 3207).
9 Amended by No I of the Ordinance of 30 June 2010, in force since 1 Aug. 2010 (AS **2010** 3207).
10 Inserted by No I of the Ordinance of 29 Oct. 2014, in force since 1 Jan. 2015 (AS **2014** 3543).
11 Amended by No I of the Ordinance of 30 June 2010, in force since 1 Aug. 2010 (AS **2010** 3207).

c. It coordinates its activities with the IT Security Committee.

d. It guarantees the provision of the information to the General Secretaries Conference.

e.[12] Every two years, it reports to the General Secretaries Conference on strategic concerns of the Information Protection Report.

f. It may consult other services.

[3] In agreement with the Departments and the Federal Chancellery, it draws up business regulations for itself and the Coordination Agency.

Art. 20*a*[13] Coordination Agency for Federal Information Protection

[1] The Coordination Committee is supported by the Coordination Agency. The latter has the following tasks:

a. It manages the secretariat of the Coordination Committee.

b. It is the central point of contact for domestic, foreign and international agencies concerned with information protection.

c. It supports the information protection delegates of the Departments and the Federal Chancellery in its field.

d. It creates the necessary training aids.

e. It may carry out the security inspections required by international treaties and further checks in consultation with the Departments and the Federal Chancellery.

[2] The Coordination Agency is assigned in administrative terms to the General Secretariat of the Federal Department of Defence, Civil Protection and Sport.[14]

Section 6 Final Provisions

Art. 21 Implementation

The Departments and the Federal Chancellery shall implement this Ordinance.

Art. 22 Repeal and amendment of current law

[1] The following are repealed:

a. Ordinance of 10 December 1990[15] on the Classification and Handling of Information from the Civilian Administrative Sector;

12 Amended by No I of the Ordinance of 1 May 2013, in force since 1 June 2013 (AS **2013** 1341).
13 Inserted by No I of the Ordinance of 30 June 2010, in force since 1 Aug.. 2010 (AS **2010** 3207).
14 Amended by Annex No 2 of the Ordinance of 3 June 2016, in force since 1 July 2016 (AS **2016** 1785).
15 [AS **1991** 44, **1999** 2424 Art. 27 No 1]

b. Ordinance of the Federal Department of Defence of 1 May 1990[16] on the Protection of Military Information (Information Protection Ordinance).

2 …[17]

Art. 23 Transitional provisions

1 The classification «INTERNAL» may only be applied to information carriers that are created after this Ordinance comes into force.

2 Technical adjustments to ensure the protection of information, in particular concerning its classification and handling, must be carried out by 31 December 2009.

Art. 24 Commencement

1 This Ordinance comes into force on 1 August 2007 and is valid until 31 December 2011 at the latest.

2 The period of validity of this Ordinance is extended until 31 December 2014.[18]

3 The period of validity of this Ordinance is extended until 31 December 2017.[19]

4 The period of validity of this Ordinance is extended until 31 December 2020.[20]

16 [AS **1990** 887, **1999** 2424 Art. 27 No 3]
17 These amendments may be consulted under AS **2007** 3401.
18 Inserted by No I of the Ordinance of 30 June 2010, in force since 1 Aug. 2010 (AS **2010** 3207).
19 Inserted by No I of the Ordinance of 29 Oct. 2014, in force since 1 Jan. 2015 (AS **2014** 3543).
20 Inserted by No I of the Ordinance of 1 Dec. 2017, in force since 1 Jan. 2018 (AS **2017** 7391).

Annex
(Art. 18 para. 1)[21]

Handling regulations

	SECRET	CONFIDENTIAL	INTERNAL	Person Responsible
Creation				
Resources (the regulations agreed on implementing the Ordinance of 29 August 1990[22] on Classification Procedure for Assignments with Classified Military Content apply.	Electronically: only with resources authorised by the Coordination Agency (exception: armed forces)	Electronically: only with resources authorised by the Coordination Agency (exception: armed forces)	Arbitrary	Author
Classification	Mark every page with: «SECRET»	Mark every page with: «CONFIDENTIAL»	Mark every page with: «INTERNAL»	
Numbering	Compulsory	Optional	None	
Registration	Coordination Agency's forms	List of recipients	Optional	
Storage or preservation				
Electronic	Only on resources authorised by the Coordination Agency; encrypted on workplace systems or encrypted on removable data carriers Keys are stored separately from the encrypted information and kept under lock and key	Encrypted on workplace systems or encrypted on removable data carriers	Accessible to authorised persons only	Author or confidant

21 See also detailed processing regulations for the Coordination Agency (Art. 18, para 2).
22 SR **510.413**

	SECRET	CONFIDENTIAL	INTERNAL	Person Responsible
Physical	Safe	Secured container	Accessible to authorised persons only	
Transfer or transmission and reception				
Telephone, mobile	Encrypted or protected transfer pathway or security concept	Encoded or encrypted	Encoded or within federal network	Author or confidant
Fax	Encryption or protected transfer pathway or security concept	Encryption or protected transfer pathway or security concept	Permitted	
E-mail (or annex thereof)	Encrypted and reproducible	Encrypted	Permitted, protection necessary, e g. federal network	
Data transmission	Encryption or protected transfer pathway	Encryption or protected transfer pathway	Permitted, protection necessary, e.g. federal network	
Oral statements	Only to authorised persons, in areas where eavesdropping is impossible			
Transmission or dispatch and reception				
Personal hand-over	Only permitted against receipt	Permitted, in the case of numbered editions against receipt only	Permitted	Author or confidant
Postal system, courier	Restricted and only permitted by special federal courier	Permitted in restricted cases, in the case of numbered editions by registered letter	Permitted in restricted cases	
Use				
Processing with IT applications (with the exception of arrangements made pertaining to secrecy protection procedures)	Only with resources authorised by the Coordination Agency and with the use of security software that satisfies federal standards	Only with resources authorised by the Coordination Agency (exception: armed forces) and with the use of security software that satisfies federal standards	Permitted	Author or confidant

	SECRET	CONFIDENTIAL	INTERNAL	Person Responsible
Printing	Permitted in restricted cases	Permitted in restricted cases	Permitted	
Copying	Restricted and exclusively permitted at the author's consent	Permitted in restricted cases	Permitted	
Removal from permanent location	Permitted in restricted cases	Permitted in restricted cases	Permitted	
Information management				
Regular evaluation of classification and recipients	At least every five years and always with due regard to obligation to offer to the Federal Archives (Art. 14)	For numbered editions only: at least every five years and always with due regard to the obligation to offer to the Federal Archives (Art. 14)	None	Author
Withdrawal and withdrawal obligation	Compulsory	Compulsory if numbered	None	Author or confidant
Archiving	Obligation to offer under the archiving legislation (Art. 17).			author or confidant
Destruction or deletion (as long as there is no deposit obligation under the archiving legislation)	Destruction by author only and Permitted in restricted cases	Permitted in restricted cases, in the case of numbered editions by author only	Permitted in restricted cases	