# Declaration by the Swiss National Bank regarding the implementation of the Federal Act on Information Security

# of 25 August 2026 (as at 1 November 2026)

## 1. General

Pursuant to art. 84 para. 3 of the Federal Act on Information Security (Information Security Act, ISA), the Federal Council's implementing provisions apply analogously to the authorities subject to the ISA, unless these authorities issue their own provisions.

This document contains the implementing provisions of the Swiss National Bank (SNB) for the ISA. In particular, it governs the SNB's implementation of the ISA requirements. Details are set out in an internal document.

## 2. Principles

The SNB ensures risk-based protection of its information and IT tools, as well as appropriate resilience to information security risks.

The SNB protects its information according to five criteria: confidentiality, integrity, availability, auditability and authenticity.

The SNB regulates the details of its information security by means of an Information Security Management System (cf. section 3).

The SNB's Information Security Officer advises and supports the relevant line managers in the fulfilment of their tasks and obligations under the ISA, is responsible for the specialist organisation of information security and associated risk management, reviews compliance with information security requirements, reports to SNB management and requests the implementation of necessary measures.

## 3. Management of information security

### 3.1 Information Security Management System (ISMS)

In particular, the ISMS sets out the methods and procedures for defining, managing, controlling and ensuring information security at the SNB, as well as responsibilities and measure-related objectives.

The ISMS is periodically reviewed with respect to completeness and effectiveness.

The detailed definition, implementation and monitoring of the measure-related objectives are handled by the SNB units responsible using specific measures. The SNB assesses compliance with these information security objectives annually. The results of the assessment are reported to SNB management.

### 3.2 Risk management methodology

The SNB keeps an inventory of its protected items, continuously assesses the risks to which these protected items are exposed and performs the following tasks in particular:

a) It regularly analyses threats and vulnerabilities and assesses their impact on the protected items.

b) It implements the necessary measures and monitors their impact.

c) It monitors compliance with external and internal requirements.

d) It accounts for the acceptance of residual risks.

Information security risks are managed in accordance with the ISMS as part of the SNB's internal control system (ICS).

### 3.3 Cooperation with third parties

The SNB assesses the risks to which its protected items are exposed when it cooperates with third parties, as well as its dependence on third parties.

As part of the procurement process, steps are taken to ensure that service provider-specific risks are consistently identified, evaluated, assessed and – where possible – managed.

### 3.4 Dealing with security incidents and vulnerabilities

The SNB determines how security incidents and vulnerabilities are to be reported and handled, and which units within the SNB can order immediate measures.

## 4. Classification of information

The disclosure and making available of classified information and the creation of classified information carriers are to be kept to a minimum (need-to-know principle).

The SNB has three classification levels: INTERNAL, CONFIDENTIAL and SECRET.

The information owner is responsible for classifying information.

Access to information is granted only to those persons who require it to perform their operational tasks. Access is to be organised using authorisations to ensure that the tasks can be performed in a targeted manner.

The SNB regulates classification details in a directive. This includes, among other things, requirements with respect to the processing of classified information, and minimum organisational, personnel-related, technical and structural requirements for its protection.

# 5. Security when using IT tools

## 5.1 Security procedures

To safeguard its protected items, the SNB carries out security procedures, consisting in particular of a protection requirements analysis, a risk analysis, residual risk acceptance, and a security measure implementation review.

The security procedures for individual protected items are repeated in the event of significant changes in the threat situation, technology, tasks or organisational conditions.

## 5.2 Security levels

The SNB regulates how IT tools are assigned to the security levels ‘baseline protection,’ ‘high protection’ or ‘very high protection’. All IT tools used at the SNB must meet the minimum requirements of the ‘baseline protection’ security level.

## 5.3 Security measures

The SNB sets the minimum requirements for the respective security levels in accordance with art. 17 ISA. In doing so, it takes account of requirements applying to the security of personal data under data protection legislation as well as the relevant requirements applying to other information that the SNB has a statutory obligation to protect.

As part of the ISMS framework, before commissioning, in the event of significant changes in risks during operation, and in the context of periodic assessments, the SNB reviews and documents the effectiveness of the measures taken for protected items assigned to the ‘very high protection’ security level.

## 5.4 Security during operation

The SNB ensures that it has the necessary personnel/financial resources and skills for early detection, technical analysis, security incident management and security vulnerability handling, as well as for monitoring the use of its IT structure.

# 6. Personnel measures and physical protection

## 6.1 Screening of personnel

In directives, the SNB sets minimum requirements for risk-based screening of personnel requiring access to information and IT tools as well as to the SNB's premises.

The SNB has four levels of personnel security screening, which differ according to the criticality of the security zone.

The SNB ensures that staff subject to personnel security screening are made aware of the relevant security-sensitive activity and associated risks on an annual basis.

## 6.2 Physical protection measures

In directives, the SNB issues minimum requirements for the physical protection of information. Admission to the SNB's premises is governed by an access policy.

The SNB's premises and areas are assigned to a security zone according to the degree of risk and accessibility. The SNB takes appropriate protection measures in each of these areas, factoring in the degree of risk involved.

| | | | |
|---|---|---|---|
| **Issued by** | Board of Deputies | **Issued on** | 25 August 2026 |
| **Entry into force** | 1 November 2026 | **Owner:** | OpRisk & Security |
| **Legal basis** | Art. 84 para. 3 Information Security Act (ISA) | | |
| **Replaces** | - | | |
| **Amended on** | **Amended by** | **Amendment valid from** | **Section(s)** |
| | | | |