Ausführungserklärung der Schweizerischen Nationalbank zur Umsetzung des Informationssicherheitsgesetzes des Bundes

vom 25. August 2026 (Stand am 1. November 2026)

1. Allgemeines

Gemäss Art. 84 Abs. 3 des Bundesgesetzes über die Informationssicherheit (Informationssicherheitsgesetz, ISG) gelten die Ausführungsbestimmungen des Bundesrats für die verpflichteten Behörden sinngemäss, sofern diese keine eigenen Vorschriften erlassen.

Dieses Dokument enthält die Ausführungsbestimmungen der Schweizerischen Nationalbank (SNB) zum ISG. Es regelt insbesondere die Umsetzung der Vorgaben des ISG durch die SNB. Einzelheiten werden in einem internen Dokument geregelt.

2. Grundsätze

Die SNB sorgt für einen risikobasierten Schutz ihrer Informationen und Informatikmittel sowie für angemessene Resilienz gegenüber Informationssicherheitsrisiken.

Die SNB schützt ihre Informationen nach den Kriterien Vertraulichkeit, Integrität, Verfügbarkeit, Nachvollziehbarkeit und Authentizität.

Die SNB regelt Einzelheiten zur Informationssicherheit mittels eines Informationssicherheits-Management-Systems (siehe Ziffer 3).

Der oder die Informationssicherheitsbeauftragte der SNB berät und unterstützt die zuständigen Linienstellen bei der Erfüllung ihrer Aufgaben und Pflichten gemäss ISG, verantwortet die Fachorganisation der Informationssicherheit sowie das entsprechende Risikomanagement, überprüft die Einhaltung der Vorgaben der Informationssicherheit, erstattet der Bankleitung Bericht und beantragt die Umsetzung der erforderlichen Massnahmen.

3. Management der Informationssicherheit

3.1 Informationssicherheits-Management-System (ISMS)

Das ISMS beschreibt insbesondere Methoden und Verfahren zur Definition, Steuerung, Kontrolle und Gewährleistung der Informationssicherheit bei der SNB sowie Verantwortlichkeiten und Massnahmenziele.

Das ISMS wird periodisch auf Vollständigkeit und Wirksamkeit hin überprüft.

Die Konkretisierung, Umsetzung und Überwachung der Massnahmenziele erfolgen mittels spezifischer Massnahmen durch die zuständigen Stellen innerhalb der SNB. Die SNB prüft jährlich die Einhaltung dieser Informationssicherheitsziele. Die Ergebnisse der Prüfung werden der Bankleitung berichtet.

3.2 Risikomanagement-Methodik

Die SNB führt ein Inventar ihrer Schutzobjekte und beurteilt laufend die Risiken für ihre Schutzobjekte und nimmt insbesondere folgende Aufgaben wahr:

a) Sie analysiert regelmässig Bedrohungen und Schwachstellen und bewertet deren Auswirkungen auf die Schutzobjekte.
b) Sie setzt die notwendigen Massnahmen um und kontrolliert deren Wirkung.
c) Sie kontrolliert die Einhaltung der externen und internen Vorgaben.
d) Sie weist die Akzeptanz der Restrisiken nach.

Das Management der Informationssicherheitsrisiken erfolgt gemäss ISMS im Rahmen des Internen Kontrollsystems (IKS) der SNB.

3.3 Zusammenarbeit mit Dritten

Die SNB beurteilt die Risiken für ihre Schutzobjekte bei der Zusammenarbeit mit Dritten und ihre Abhängigkeit von Dritten.

Im Rahmen des Beschaffungsprozesses wird sichergestellt, dass eine einheitliche Identifikation, Bewertung, Beurteilung und mögliche Bewirtschaftung von dienstleisterspezifischen Risiken erfolgt.

3.4 Vorgehen bei Sicherheitsvorfällen und Sicherheitslücken

Die SNB legt fest, wie Sicherheitsvorfälle und Sicherheitslücken gemeldet und behandelt werden und welche Stellen in der SNB Sofortmassnahmen anordnen können.

4. Klassifizierung von Informationen

Die Bekanntgabe und das Zugänglichmachen von klassifizierten Informationen sowie die Erstellung klassifizierter Informationsträger sind auf das Minimum zu beschränken («Need-to-Know»-Prinzip).

Die SNB unterscheidet die drei Klassifizierungsstufen INTERN, VERTRAULICH und GEHEIM.

Die Informationseignerin ist für die Klassifizierung von Informationen zuständig.

Zugriff auf Informationen erhalten nur Personen, die diesen zur Erfüllung ihrer betrieblichen Aufgabe benötigen. Der Zugriff ist mittels Berechtigungen so zu gestalten, dass die Aufgabenerfüllung zielgerichtet erfolgen kann.

Die SNB regelt Einzelheiten zur Klassifizierung in einer Weisung. Diese enthält u.a. Vorgaben zur Bearbeitung klassifizierter Informationen und organisatorische, personelle, technische und bauliche Mindestanforderungen für deren Schutz.

5. Sicherheit beim Einsatz von Informatikmitteln

5.1 Sicherheitsverfahren

Zum Schutz ihrer Schutzobjekte führt die SNB Sicherheitsverfahren durch, die insbesondere aus einer Schutzbedarfsanalyse, Risikoanalyse, Akzeptanz der Restrisiken und Prüfung der Umsetzung der Sicherheitsmassnahmen bestehen.

Die Wiederholung der Sicherheitsverfahren einzelner Schutzobjekte erfolgt bei wesentlichen Änderungen der Bedrohung, Technologie, Aufgaben oder Organisationsverhältnisse.

5.2 Sicherheitsstufen

Die SNB regelt die Zuordnung der Informatikmittel zu den Sicherheitsstufen «Grundschutz», «hoher Schutz» oder «sehr hoher Schutz». Alle in der SNB eingesetzten Informatikmittel müssen die Mindestanforderungen der Sicherheitsstufe «Grundschutz» erfüllen.

5.3 Sicherheitsmassnahmen

Die SNB legt die Mindestanforderungen für die jeweiligen Sicherheitsstufen nach Artikel 17 ISG fest. Sie berücksichtigt dabei die Anforderungen für die Sicherheit von Personendaten nach der Datenschutzgesetzgebung sowie betreffend andere Informationen, welche die SNB aufgrund gesetzlicher Verpflichtungen schützen muss, die jeweiligen gesetzlichen Vorgaben.

Im Rahmen des ISMS prüft und dokumentiert die SNB vor der Inbetriebnahme, bei wesentlichen Änderungen der Risiken während des Betriebs sowie im Rahmen periodischer Prüfungen die Wirksamkeit der Massnahmen von Schutzobjekten der Sicherheitsstufe «sehr hoher Schutz».

5.4 Sicherheit beim Betrieb

Die SNB stellt sicher, dass sie über die nötigen personellen und finanziellen Kapazitäten und Fähigkeiten zur frühzeitigen Entdeckung, technischen Analyse, Bewältigung von Sicherheitsvorfällen, Behandlung von Sicherheitslücken und Überwachung der Nutzung ihrer Informatikstruktur verfügt.

6. Personelle Massnahmen und physischer Schutz

6.1 Prüfung von Personen

Die SNB erlässt in Weisungen Mindestanforderungen an die risikobasierte Prüfung von Personen, die Zugriff auf Informationen und Informatikmittel sowie Zugang zu Räumlichkeiten der SNB benötigen.

Die SNB unterscheidet bei Personensicherheitsprüfungen zwischen vier Stufen. Diese unterscheiden sich nach der Kritikalität der entsprechenden Sicherheitszone.

Die SNB stellt sicher, dass Mitarbeitende, die einer Personensicherheitsprüfung unterliegen, jährlich für die massgebende sicherheitsempfindliche Tätigkeit und die entsprechenden Risiken sensibilisiert werden.

6.2 Physische Schutzmassnahmen

Die SNB erlässt in Weisungen Mindestanforderungen für den physischen Schutz von Informationen. Ein Zutrittskonzept regelt den Zugang zu den Räumlichkeiten der SNB.

Die Räumlichkeiten und Bereiche der SNB werden abgestuft nach Gefährdungsgrad und Zutrittsmöglichkeit einer Sicherheitszone zugeordnet. Die SNB trifft für jeden dieser Bereiche unter Berücksichtigung des jeweiligen Gefährdungsgrades angemessene Schutzmassnahmen.

Erlassen durch:	Kollegium der Stellvertreterinnen und Stellvertreter	**Erlassen am:**	25.08.2026
Inkraftsetzung:	01.11.2026	**Eigner:**	OpRisk & Sicherheit
Rechtsgrundlage:	Art. 84 Abs. 3 Informationssicherheitsgesetz (ISG)		
Ersetzt:	–		
Geändert am:	**Geändert durch:**	**Änderung gültig per:**	**Ziffer(n):**