Dispositions d'exécution édictées par la Banque nationale suisse concernant la mise en œuvre de la loi fédérale sur la sécurité de l'information

du 25 août 2026 (état le 1er novembre 2026)

1. Généralités

En vertu de l'art. 84, al. 3 de la loi fédérale sur la sécurité de l'information (loi sur la sécurité de l'information, LSI), les dispositions d'exécution du Conseil fédéral s'appliquent par analogie aux autorités soumises à la LSI pour autant que ces dernières n'édictent pas leurs propres dispositions.

Le présent document contient les dispositions d'exécution définies par la Banque nationale suisse (BNS) pour mettre en œuvre la LSI. Les modalités détaillées sont réglées séparément.

2. Principes

La BNS veille à protéger ses informations et ses moyens informatiques en fonction du risque et à faire preuve d'une résilience appropriée face aux risques pour la sécurité de l'information.

La BNS protège ses informations sur la base des critères suivants: confidentialité, intégrité, disponibilité, traçabilité et authenticité.

La BNS fixe les règles détaillées relatives à la sécurité de l'information au moyen d'un système de management de la sécurité de l'information (voir chiffre 3).

La personne préposée à la sécurité de l'information de la BNS conseille et aide les responsables hiérarchiques dans l'accomplissement des tâches et dans l'exécution des obligations qui leur incombent en vertu de la LSI. Elle est également responsable de l'organisation de la sécurité de l'information sur le plan technique et de la gestion des risques qui s'y rapportent, veille à ce que les prescriptions relatives à la sécurité de l'information soient respectées, en rend compte à la direction de la Banque et propose les mesures nécessaires.

3. Gestion de la sécurité de l’information

3.1 Système de management de la sécurité de l’information (SMSI)

Le SMSI décrit notamment les méthodes et les processus utilisés pour définir, piloter, contrôler et assurer la sécurité de l’information à la BNS. Il décrit également les responsabilités et les objectifs visés par les mesures mises en œuvre.

L’exhaustivité et l’efficacité du SMSI font l’objet de contrôles réguliers.

Il incombe aux unités responsables, au sein de la BNS, de définir les objectifs visés et d’assurer et de surveiller leur réalisation au moyen de mesures spécifiques. La réalisation des objectifs est contrôlée chaque année, et la direction de la Banque est informée des résultats.

3.2 Méthode de gestion des risques

La BNS dresse un inventaire des objets à protéger, évalue en continu les risques auxquels sont exposés ces objets et assume notamment les tâches suivantes:

a) elle analyse régulièrement les menaces et les vulnérabilités, et en évalue les répercussions sur les objets à protéger;

b) elle met en œuvre les mesures nécessaires et en contrôle les effets;

c) elle contrôle le respect des prescriptions internes et externes;

d) elle démontre l’acceptation des risques résiduels.

Comme le prévoit le SMSI, la gestion des risques liés à la sécurité de l’information se fait dans le cadre du système de contrôle interne (SCI) de la BNS.

3.3 Collaboration avec les tiers

La BNS évalue les risques pour ses objets à protéger lors de la collaboration avec des tiers et sa dépendance vis-à-vis de tiers.

Dans le cadre du processus régissant les achats, elle veille à ce que les risques spécifiques aux prestataires de services soient identifiés, analysés, évalués et, dans la mesure du possible, gérés de manière uniforme.

3.4 Procédure à suivre en cas d’incidents et de failles de sécurité

La BNS fixe la manière dont les incidents et les failles de sécurité sont annoncés et traités. Elle détermine également les unités habilitées à ordonner des mesures immédiates.

4. Classification des informations

La communication et la mise à disposition d'informations classifiées et la création de supports d'information classifiés doivent être limitées au strict nécessaire (principe du besoin d'en connaître ou *need to know*).

La BNS distingue trois échelons de classification: «INTERNE», «CONFIDENTIEL» et «SECRET».

La classification des informations incombe aux personnes qui en sont propriétaires.

L'accès aux informations est réservé aux personnes qui en ont besoin pour accomplir leurs tâches opérationnelles. Il doit être défini à l'aide de droits d'accès de telle sorte que les tâches puissent être effectuées de manière ciblée (principe du besoin d'en connaître).

La BNS fixe les règles détaillées relatives à la classification des informations dans une directive. Cette dernière définit notamment les prescriptions au sujet du traitement des informations classifiées et les exigences de protection minimales sur le plan technique ainsi qu'en matière d'organisation, de personnel et de construction.

5. Sécurité des moyens informatiques

5.1 Procédure de sécurité

Pour ses objets à protéger, la BNS met en œuvre des procédures de sécurité comprenant notamment une analyse des besoins en protection, une analyse des risques, l'acceptation des risques résiduels et l'examen de la mise en œuvre des mesures de sécurité.

La procédure de sécurité pour les objets à protéger est répétée en cas de changements importants concernant la menace, la technologie, les tâches ou la situation de l'organisation.

5.2 Catégories de sécurité

La BNS réglemente la classification des moyens informatiques dans les catégories de sécurité «protection de base», «protection élevée» et «protection très élevée». Tous les moyens informatiques utilisés à la BNS doivent remplir les exigences minimales de la catégorie «protection de base».

5.3 Mesures de sécurité

La BNS fixe les exigences minimales pour chaque catégorie de sécurité conformément à l'art. 17 LSI. Elle tient compte des exigences concernant la sécurité des données personnelles au sens de la législation sur la protection des données et la sécurité des autres informations qu'elle doit protéger en vertu de ses obligations légales.

Dans le cadre du SMSI, la BNS contrôle et documente l'efficacité des mesures applicables aux objets à protéger relevant de la catégorie de sécurité «protection très élevée» avant leur mise en exploitation, en cas de changements importants des risques durant l'exploitation et dans le cadre de vérifications périodiques.

5.4 Sécurité de l'exploitation

La BNS veille à disposer, sur le plan du personnel et des finances, des capacités et compétences nécessaires à la détection précoce, à l'analyse technique, à la maîtrise des incidents de sécurité, au traitement des failles de sécurité et à la surveillance de l'utilisation de son infrastructure informatique.

6. Mesures relatives aux personnes et protection physique

6.1 Vérification de l'identité des personnes

Par voie de directive, la BNS émet des prescriptions qui concernent les exigences minimales auxquelles doit satisfaire la vérification, en fonction du risque, de l'identité des personnes qui ont besoin d'accéder à des informations, à des moyens informatiques ou à des locaux de la BNS.

La BNS distingue quatre niveaux de contrôle de sécurité relatifs aux personnes. Ces niveaux dépendent du caractère plus ou moins sensible de la zone de sécurité concernée.

La BNS veille à ce que les collaboratrices et collaborateurs soumis à un contrôle de sécurité relatif aux personnes soient chaque année rendus attentifs au caractère sensible de l'activité déterminante et aux risques qui y sont liés.

6.2 Mesures de protection physique

Par voie de directive, la BNS émet des prescriptions qui concernent les exigences minimales en matière de protection physique des informations. La politique en matière d'accès régit l'accès aux locaux de la BNS.

Les locaux et les espaces de la BNS sont classés en fonction du degré de vulnérabilité que présente une zone de sécurité et de ses possibilités d'accès. La BNS prend des mesures de protection appropriées pour chacun de ces espaces en tenant compte du degré de vulnérabilité qu'ils présentent.

Édicté par:	Collège des suppléantes et suppléants	**Édicté le:**	25.08.2026
Entré en vigueur:	01.11.2026	**Auteur:**	Risques opérationnels et sécurité
Fondements juridiques:	Art. 84, al. 3 de la loi sur la sécurité de l'information (LSI)		
Remplace:	–		
Modifié le:	**Modifié par:**	**En vigueur depuis le:**	**Chiffre(s):**