Ordonnance sur la sécurité de l'information dans l'administration fédérale et l'armée

(Ordonnance sur la sécurité de l'information, OSI)

du 8 novembre 2023 (État le 1er mai 2025)

Le Conseil fédéral suisse,

vu les art. 2, al. 3 et 4, 12, al. 3, 83, al. 3, 84, al. 1, 85, al. 1 et 2, et 86, al. 4, de la loi du 18 décembre 2020 sur la sécurité de l'information (LSI)[1],

arrête:

Section 1 Dispositions générales

Art. 1 Objet
(art. 1 LSI)

La présente ordonnance régit les tâches, les responsabilités, les compétences et les procédures qui permettent de garantir la sécurité de l'information au sein de l'administration fédérale et de l'armée.

Art. 2 Champ d'application
(art. 2 et 3 LSI)

1 La présente ordonnance s'applique:

a. au Conseil fédéral;

b. aux départements;

c. à la Chancellerie fédérale (ChF), aux secrétariats généraux, aux groupements et aux offices fédéraux;

d. à l'armée.

2 Les dispositions suivantes de la LSI et de la présente ordonnance s'appliquent aux unités de l'administration fédérale décentralisée au sens de l'art. 2, al. 3, de la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA)[2] et aux organisations et personnes visées à l'art. 2, al. 4, LOGA:[3]

a. les art. 5, 6, 9, 10, 12 à 15, 20 à 23 et 27 à 73 LSI et les art. 16, 21, 24, 26, 32, 34 et 35 de la présente ordonnance, lorsqu'elles traitent des informations classifiées de la Confédération;

RO **2023** 735

1 RS **128**
2 RS **172.010**
3 Nouvelle teneur selon l'annexe 2 ch. II 1 de l'O du 2 avr. 2025 sur la numérisation, en vigueur depuis le 1er mai 2025 (RO **2025** 235).

b.[4] les art. 5, 6, 9, 10 et 16 à 73 LSI et 10 à 12, 27 et 29 à 35 de la présente ordonnance, lorsqu'elles accèdent aux moyens informatiques des fournisseurs internes de prestations informatiques visés à l'art. 10 de l'ordonnance du 2 avril 2025 sur la numérisation (ONum)[5] ou délèguent l'exploitation de leurs moyens informatiques à ces fournisseurs.

[3] La ChF et les départements peuvent, dans leur domaine de compétence, soumettre les unités de l'administration fédérale décentralisée qui exercent constamment des activités sensibles à l'ensemble des dispositions de la LSI.

[4] Les dispositions suivantes de la présente ordonnance s'appliquent aux cantons, sous réserve de l'art. 3, al. 2, LSI:

a. les dispositions de la section 4, lors du traitement d'informations classifiées de la Confédération;

b. les art. 28 à 30 et 34, lors de l'accès aux moyens informatiques de la Confédération.

[5] Le Groupement Défense assume pour l'armée les tâches, compétences et responsabilités que la présente ordonnance assigne aux unités administratives visées à l'art. 2, al. 1, let. c.

Section 2 Principes

Art. 3 Objectifs de sécurité
(art. 7, al. 2, let. a, LSI)

[1] Les organisations visées à l'art. 2, al. 1, veillent ensemble à protéger leurs informations et leurs moyens informatiques en fonction du risque et à faire preuve d'une résilience appropriée face aux risques pour la sécurité de l'information.

[2] Elles contribuent, en collaborant et en échangeant des informations avec les autres autorités fédérales, les cantons, les communes, les milieux économiques, la société, les milieux scientifiques et les partenaires internationaux, à améliorer la sécurité de l'information de la Suisse.

[3] Elles œuvrent à l'harmonisation, sur le plan national et international, des prescriptions et des niveaux en matière de sécurité afin de permettre l'interaction des autorités fédérales avec d'autres autorités de la Confédération ainsi qu'avec les cantons, les communes et les partenaires internationaux.

Art. 4 Responsabilité

[1] Les unités administratives sont responsables de la protection des informations qu'elles traitent ou dont elles délèguent le traitement et de la sécurité des moyens informatiques qu'elles exploitent elles-mêmes ou font exploiter par des tiers.

4 Nouvelle teneur selon l'annexe 2 ch. II 1 de l'O du 2 avr. 2025 sur la numérisation, en vigueur depuis le 1er mai 2025 (RO **2025** 235).
5 RS **172.019.1**

2 Elles assument toutes les tâches relevant de leur domaine de compétence que la présente ordonnance ou d'autres dispositions du droit fédéral n'attribuent pas à une autre organisation ou à un autre service.

3 Les collaborateurs de l'administration fédérale et les militaires qui traitent des informations ou utilisent des moyens informatiques de la Confédération sont responsables du respect des prescriptions en la matière.

4 Les supérieurs de tous les échelons sont responsables de la formation liée à la sécurité de l'information de leurs collaborateurs et des militaires qui leur sont subordonnés en fonction de leurs tâches et s'assurent que ceux-ci respectent les prescriptions.

Section 3 Gestion de la sécurité de l'information

Art. 5 Système de management de la sécurité de l'information
(art. 7, al. 1, LSI)

1 Les unités administratives visées à l'art. 2, al. 1, let. c, établissent chacune un système de management de la sécurité de l'information (SMSI).

2 Elles fixent les objectifs de leur SMSI, vérifient chaque année si ces objectifs ont été atteints et relèvent les indicateurs nécessaires à cette fin.

3 Elles font contrôler leur SMSI au moins tous les trois ans par un service indépendant ou par leur département et veillent à améliorer continuellement le système.

4 Elles coordonnent leur SMSI avec la gestion ordinaire des risques, la gestion de la continuité des activités et la gestion des crises.

Art. 6 Gestion des bases légales et des obligations contractuelles
(art. 7, al. 1, LSI)

Les unités administratives visées à l'art. 2, al. 1, let. c, les départements et le service spécialisé de la Confédération pour la sécurité de l'information établissent la liste des bases légales déterminantes pour leur domaine de compétence et de leurs obligations contractuelles en matière de sécurité de l'information et la tiennent à jour.

Art. 7 Inventaire des objets à protéger
(art. 7, al. 1, LSI)

1 Les unités administratives visées à l'art. 2, al. 1, let. c, dressent l'inventaire de leurs objets à protéger et le tiennent à jour.

2 Par objets à protéger, on entend des objets indépendants, plusieurs objets de même nature ou des objets connexes:

a. les collections d'informations traitées dans le but d'exécuter un processus d'affaires de la Confédération;

b. les moyens informatiques visés à l'art. 5, let. a, LSI.

3 L'inventaire mentionne:

a. le besoin de protection des objets à protéger;

b. les responsabilités liées aux objets à protéger;

c. la participation de tiers;

d. le résultat de l'évaluation des risques;

e. la mise en œuvre des mesures de sécurité et l'acceptation des risques qui ne peuvent pas être réduits de manière suffisante (risques résiduels);

f. les contrôles et les audits périodiques;

g. le cas échéant, l'utilisation partagée des objets à protéger.

Art. 8 Gestion des risques
(art. 7, al. 2, let. b, et 8 LSI)

1 Les unités administratives visées à l'art. 2, al. 1, let. c, évaluent en continu les risques pour leurs objets à protéger et assument notamment les tâches suivantes:

a. elles analysent régulièrement les menaces et les vulnérabilités et en évaluent les répercussions sur les objets à protéger;

b. elles mettent en œuvre les mesures nécessaires et en contrôlent les effets;

c. elles contrôlent le respect des directives;

d. elles démontrent l'acceptation des risques résiduels.

2 Le service spécialisé de la Confédération pour la sécurité de l'information, l'Office fédéral de la cybersécurité (OFCS), les unités administratives qui fournissent des prestations et les organes de sécurité de la Confédération informent les unités administratives visées à l'art. 2, al. 1, let. c, et les départements des menaces et vulnérabilités actuelles et des risques qui les concernent. Ils recommandent au besoin des mesures de limitation des risques.

3 Les unités administratives visées à l'art. 2, al. 1, let. c, rendent compte de leurs risques pour la sécurité de l'information dans le cadre du processus ordinaire de gestion des risques conformément aux directives de l'Administration fédérale des finances.

Art. 9 Autorisation et liste des exceptions
(art. 7, al. 1, LSI)

1 Si une unité administrative n'est pas en mesure d'observer une consigne contraignante pour elle d'une directive générale et abstraite visée à l'art. 85 LSI concernant un objet à protéger, elle doit obtenir une autorisation exceptionnelle du service ayant émis la directive.

2 Si une exception relevant du domaine de compétence du service spécialisé de la Confédération pour la sécurité de l'information concerne également des directives de

la ChF sur la transformation numérique et la gouvernance de l'informatique, le service spécialisé consulte au préalable le délégué TNI.[6]

3 Les unités administratives visées à l'art. 2, al. 1, let. c, les départements et le service spécialisé de la Confédération pour la sécurité de l'information établissent la liste de leurs autorisations exceptionnelles en vigueur.

Art. 10 Collaboration avec les tiers
(art. 9 LSI)

1 Les unités administratives visées à l'art. 2, al. 1, let. c, évaluent les risques pour leurs objets à protéger lors de la collaboration avec des tiers et leur dépendance vis-à-vis de tiers.

2 Les services d'achat centraux visés à l'art. 5 de l'ordonnance du 1er mai 2024 sur l'organisation des marchés publics de l'administration fédérale (Org-OMP)[7] collaborent à l'évaluation et mettent les informations nécessaires à disposition.[8]

3 Le service spécialisé de la Confédération pour la sécurité de l'information, après avoir consulté l'OFCS et la Conférence des achats de la Confédération visée à l'art. 30 Org OMP, émet des recommandations quant aux dispositions relatives à la sécurité de l'information devant figurer dans tous les contrats d'acquisition ou de prestation de la Confédération.[9]

Art. 11 Formation et sensibilisation
(art. 7, al. 1, et 20, al. 1, let. c, LSI)

1 Les unités administratives visées à l'art. 2, al. 1, let. c, forment leurs collaborateurs à leur entrée en fonction, puis périodiquement de manière à ce qu'ils puissent assumer leurs responsabilités en matière de sécurité de l'information. Elles établissent la liste des formations et des participants.

2 Les formations portent notamment sur:

a. l'identification correcte du besoin de protection des informations;

b. l'utilisation sûre des informations et des moyens informatiques;

c. la réaction correcte en cas de soupçon d'incident de sécurité;

d. la connaissance de l'organisation de sécurité et des interlocuteurs en cas de questions relatives à la sécurité de l'information;

e. les tâches de contrôle des supérieurs;

6 Nouvelle teneur selon l'annexe 2 ch. II 1 de l'O du 2 avr. 2025 sur la numérisation, en vigueur depuis le 1er mai 2025 (RO **2025** 235).
7 RS **172.056.15**
8 Nouvelle teneur selon l'art. 44 al. 2 ch. 1 de l'O du 1er mai 2024 sur l'organisation des marchés publics de l'administration fédérale, en vigueur depuis le 1er juil. 2024 (RO **2024** 224).
9 Nouvelle teneur selon l'art. 44 al. 2 ch. 1 de l'O du 1er mai 2024 sur l'organisation des marchés publics de l'administration fédérale, en vigueur depuis le 1er juil. 2024 (RO **2024** 224).

f. la mise en œuvre de la sécurité de l'information dans les projets et dans l'exploitation.

3 Les unités administratives visées à l'art. 2, al. 1, let. c, les départements et le service spécialisé de la Confédération pour la sécurité de l'information veillent à sensibiliser régulièrement les collaborateurs de tous les échelons aux risques pour la sécurité de l'information.

4 Le service spécialisé de la Confédération pour la sécurité de l'information établit des outils de formation et de sensibilisation.

Art. 12 Gestion des incidents
(art. 7, al. 1, et 10, al. 1, LSI)

1 Les unités administratives visées à l'art. 2, al. 1, let. c, fixent en accord avec leurs fournisseurs de prestations la manière dont les incidents et les failles de sécurité sont annoncés et maîtrisés ou traités. Elles règlent la compétence d'ordonner des mesures immédiates.

2 Si un fournisseur de prestations découvre des incidents ou des failles de sécurité qui concernent une unité administrative à laquelle il fournit des prestations, il les lui annonce immédiatement et l'aide à les maîtriser ou à les traiter.

3 Le service spécialisé de la Confédération pour la sécurité de l'information et l'OFCS peuvent aider les unités administratives visées à l'art. 2, al. 1, let. c, et les départements à maîtriser les incidents de sécurité et à traiter les failles de sécurité.

4 Les unités administratives visées à l'art. 2, al. 1, let. c, vérifient lors de la maîtrise des incidents de sécurité s'il est nécessaire de faire une annonce au Préposé fédéral à la protection des données et à la transparence en vertu de la législation sur la protection des données.

5 Elles informent immédiatement leur département et le service spécialisé de la Confédération pour la sécurité de l'information de l'incident ou de la faille de sécurité si l'une des conditions suivantes est remplie:

a. le fonctionnement de l'administration fédérale pourrait être compromis;

b. un moyen informatique relevant des catégories de sécurité «protection élevée» ou «protection très élevée» est concerné;

c. plusieurs départements pourraient être touchés;

d. la protection des informations classifiées d'un État ou d'une organisation internationale avec lequel ou laquelle le Conseil fédéral a conclu un traité international visé à l'art. 87 LSI pourrait être menacée;

e. l'incident ou la faille de sécurité pourrait avoir une grande importance politique;

f. l'incident ou la faille de sécurité requiert des mesures sortant de la procédure fixée à l'al. 1.

6 Le service spécialisé de la Confédération pour la sécurité de l'information évalue le risque et le soutien requis avec l'unité administrative concernée.

7 Dans les cas visés à l'al. 5, il peut, en accord avec l'unité administrative et le département concernés, diriger les opérations de maîtrise de l'incident de sécurité ou de traitement de la faille de sécurité ou en déléguer la direction à l'OFCS avec son approbation. Ils ont dans ce cadre les tâches et les compétences suivantes:

a. ils peuvent obliger les unités administratives, les fournisseurs de prestations et les tiers concernés à leur communiquer toutes les informations nécessaires;

b. ils peuvent ordonner des mesures immédiates;

c. ils peuvent demander l'aide de spécialistes externes;

d. ils informent la direction des unités administratives concernées et des départements de l'avancement des opérations.

8 Lorsque la sécurité de l'information a été rétablie à la suite d'un incident ou d'une faille de sécurité et que les travaux de suivi nécessaires et leur financement ont été arrêtés, le service spécialisé de la Confédération pour la sécurité de l'information ou l'OFCS rend la direction des opérations à l'unité administrative concernée.

Art. 13 Planification des contrôles et des audits

(art. 7, al. 1, 81, al. 2, let. c, et 83, al. 1, let. c, LSI)

1 Les unités administratives visées à l'art. 2, al. 1, let. c, et les départements fixent dans une planification annuelle de contrôle et d'audit la manière de contrôler en fonction du risque le respect des prescriptions de la présente ordonnance et l'efficacité des mesures permettant de garantir la sécurité de l'information dans leur domaine de compétence et auprès des tiers mandatés.

2 Les audits menés auprès des tiers disposant d'une déclaration de sécurité relative aux entreprises visée à l'art. 61 LSI doivent être coordonnés avec le service spécialisé chargé de mener la procédure de sécurité relative aux entreprises.

3 Le service spécialisé de la Confédération pour la sécurité de l'information recueille le besoin de contrôle et d'audit pour garantir la sécurité de l'information de l'ensemble de l'administration fédérale et de l'armée.

4 Il peut, en accord avec la ChF ou le département responsable, réaliser des audits ou en confier la réalisation au Contrôle fédéral des finances.

Art. 14 Compte rendu

(art. 7, al. 1, 81, al. 2, let. c, et 83, al. 1, let. h, LSI)

1 La ChF, les départements, l'OFCS et les fournisseurs internes de prestations informatiques visés à l'art. 10 ONum[10] rendent compte chaque année au service spécialisé de la Confédération pour la sécurité de l'information de la situation en matière de sécurité de l'information dans leur domaine de compétence. Ils collectent les informations nécessaires auprès des unités administratives et de leurs fournisseurs de prestations.[11]

10 RS **172.019.1**

11 Nouvelle teneur selon l'annexe 2 ch. II 1 de l'O du 2 avr. 2025 sur la numérisation, en vigueur depuis le 1er mai 2025 (RO **2025** 235).

2 Le service spécialisé de la Confédération pour la sécurité de l'information rend compte chaque année au Conseil fédéral de la situation en matière de sécurité de l'information au sein de la Confédération.

3 Il coordonne les comptes rendus avec les autorités visées à l'art. 2, al. 1, LSI.

Art. 15 Directives relatives à la gestion de la sécurité de l'information
(art. 85 LSI)

Le service spécialisé de la Confédération pour la sécurité de l'information émet des directives générales et abstraites s'appliquant à toutes les organisations visées à l'art. 2, al. 1 et 3, qui concernent les exigences minimales auxquelles la gestion de la sécurité de l'information visée aux art. 5 à 14 doit répondre.

Section 4 Informations classifiées

Art. 16 Principes
(art. 11 et 14 LSI)

1 La communication et la mise à disposition d'informations classifiées et l'établissement de supports d'information classifiés doivent être limités autant que possible.

2 Si des informations sont regroupées dans un recueil, il faut réévaluer la classification.

Art. 17 Auteurs de la classification
(art. 12 LSI)

1 Les unités administratives visées à l'art. 2, al. 1, let. c, et les départements fixent dans un catalogue de classification la manière de classifier les informations souvent traitées dans leur domaine de compétence et la durée de la classification.

2 Le service spécialisé de la Confédération pour la sécurité de l'information contrôle les catalogues de classification et émet si nécessaire une recommandation.

3 Après avoir consulté la Conférence des préposés à la sécurité de l'information, il fixe dans des directives générales et abstraites s'appliquant à toutes les organisations visées à l'art. 2, al. 1 à 3, la manière de classifier les informations souvent traitées par plusieurs départements et la durée de la classification.

4 Les personnes et les services suivants sont compétents pour classifier et déclassifier les informations qui ne figurent pas dans les catalogues de classification:

a. le personnel de la Confédération et les militaires;

b. les adjudicateurs, lorsque des informations de la Confédération sont traitées par des tiers.

5 Le personnel de la Confédération, les militaires et les tiers sont compétents pour marquer formellement les supports d'information qu'ils établissent ou les informations qu'ils communiquent oralement.

Art. 18 Échelon de classification «interne»
(art. 13, al. 1, LSI)

1 Les informations susceptibles de nuire de la manière suivante aux intérêts définis à l'art. 1, al. 2, let. a à d, LSI si elles sont portées à la connaissance d'une personne non autorisée sont classifiées «interne»:

a. un important processus d'affaires du Conseil fédéral ou de l'administration fédérale ou un processus de conduite important de l'armée est entravé;

b. l'exécution d'engagements des autorités de poursuite pénale, du Service de renseignement de la Confédération (SRC), de l'armée ou des autres organes de sécurité de la Confédération est entravée;

c. des personnes subissent des lésions corporelles;

d. la sécurité nucléaire ou la sûreté d'installations nucléaires ou de matières nucléaires sont indirectement compromises;

e. la Suisse subit un désavantage sur les plans de la politique extérieure ou de l'économie;

f. les relations entre la Confédération et les cantons ou entre les cantons sont perturbées.

2 Sont également classifiées «interne» les informations permettant de tirer des conclusions sur des informations classifiées «confidentiel» ou «secret» si elles sont portées à la connaissance d'une personne non autorisée.

Art. 19 Échelon de classification «confidentiel»
(art. 13, al. 2, LSI)

Les informations susceptibles de nuire considérablement de la manière suivante aux intérêts définis à l'art. 1, al. 2, let. a à d, LSI si elles sont portées à la connaissance d'une personne non autorisée sont classifiées «confidentiel»:

a. la capacité de décision et d'action du Conseil fédéral, du Parlement, de plusieurs unités administratives ou de plusieurs corps de troupe de l'armée sont entravées durant plusieurs jours;

b. l'exécution d'opérations des autorités de poursuite pénale, du SRC, de l'armée ou des autres organes de sécurité de la Confédération conforme aux objectifs est compromise;

c. les moyens et les méthodes opérationnels des services de renseignement et des autorités de poursuite pénale de la Confédération ou l'identité de sources et de personnes exposées sont divulgués;

d. la sécurité de la population est compromise durant plusieurs jours ou des personnes ou des groupes de personnes meurent;

e. la sécurité nucléaire ou la sûreté d'installations nucléaires ou de matières nucléaires sont compromises;

f. l'approvisionnement économique du pays ou l'exploitation d'infrastructures critiques sont entravés;

g. la Suisse subit un désavantage considérable sur les plans de la politique extérieure ou de l'économie ou les relations diplomatiques avec un État ou avec une organisation internationale sont rompues;

h. la position de la Suisse est temporairement considérablement affaiblie lors de négociations relatives à des affaires importantes de politique extérieure.

Art. 20 Échelon de classification «secret»
(art. 13, al. 3, LSI)

Les informations susceptibles de nuire gravement de la manière suivante aux intérêts définis à l'art. 1, al. 2, let. a à d, LSI si elles sont portées à la connaissance d'une personne non autorisée sont classifiées «secret»:

a. la capacité de décision et d'action du Conseil fédéral, du Parlement, de plusieurs unités administratives ou de plusieurs corps de troupe de l'armée sont annihilées durant des jours ou entravées pendant des semaines;

b. l'exécution d'opérations d'importance stratégique des autorités de poursuite pénale, du SRC, de l'armée ou des autres organes de sécurité de la Confédération est compromise ou entravée durant des jours dans une mesure particulièrement importante;

c. des sources stratégiques, l'identité de personnes particulièrement exposées ou les moyens et les méthodes stratégiques des services de renseignement et des autorités de poursuite pénale de la Confédération sont divulgués;

d. la sécurité de la population est compromise durant des semaines dans une mesure particulièrement importante ou un grand nombre de personnes meurent;

e. la sécurité nucléaire ou la sûreté d'installations nucléaires ou de matières nucléaires sont compromises dans une mesure particulièrement importante;

f. l'approvisionnement économique du pays ou l'exploitation d'infrastructures critiques ne sont plus assurés durant des jours;

g. la Suisse subit durant des semaines des conséquences particulièrement lourdes sur les plans de la politique extérieure ou de l'économie, telles que des mesures d'embargo ou des sanctions;

h. la position de la Suisse est affaiblie lors de négociations relatives à des affaires stratégiques de politique extérieure durant des années.

Art. 21 Directives relatives au traitement
(art. 6, al. 2, 84, al. 1, et 85 LSI)

[1] Le service spécialisé de la Confédération pour la sécurité de l'information émet des directives générales et abstraites s'appliquant à toutes les organisations visées à l'art. 2, al. 1 à 3, qui concernent le traitement des informations classifiées et fixe les exigences de sécurité minimales en matière d'organisation, de personnel et de construction, de même que sur le plan technique. Il tient compte pour ce faire des normes internationales en la matière.

2 Il consulte au préalable les services suivants:

a. l'OFCS;

b. le service cryptographique de l'armée;

c.[12] l'Office fédéral de l'armement (armasuisse);

d. les organes de l'administration fédérale et de l'armée responsables de la sécurité des objets.

3 La ChF règle le traitement des affaires classifiées du Conseil fédéral.

4 Le traitement des informations classifiées provenant de l'étranger est régi par les prescriptions correspondant à l'échelon de classification étranger. Les dispositions différentes figurant dans un traité international visé à l'art. 87 LSI sont réservées.

Art. 22 Mesures de sécurité liées à l'engagement
(art. 6, al. 2, et 85 LSI)

1 Si des informations classifiées sont traitées dans le cadre d'un engagement ou d'une opération et ne sont accessibles qu'à un cercle fermé d'utilisateurs clairement identifiable, les personnes suivantes peuvent, après avoir consulté le service spécialisé de la Confédération pour la sécurité de l'information, arrêter des directives spécifiques à l'engagement ou à l'opération visant à simplifier le traitement:

a. le directeur de l'Office fédéral de la police;

b. le directeur du SRC;

c. le chef de l'armée;

d. le chef du commandement des Opérations;

e. le directeur de l'Office fédéral de la douane et de la sécurité des frontières.

2 Les personnes visées à l'al. 1 veillent à ce qu'il soit clairement indiqué sur les supports d'information que les prescriptions de traitement simplifié s'appliquent.

3 Les directives relatives au traitement visées à l'art. 21 s'appliquent en dehors du cercle d'utilisateurs et à la conservation des informations en vue de leur archivage.

Art. 23 Certification de sécurité des moyens informatiques
(art. 83, al. 1, let. e, LSI)

1 Les moyens informatiques sont certifiés sur le plan de la sécurité avant leur mise en exploitation si cela est nécessaire à la collaboration nationale ou internationale.

12 Nouvelle teneur selon l'art. 44 al. 2 ch. 1 de l'O du 1er mai 2024 sur l'organisation des marchés publics de l'administration fédérale, en vigueur depuis le 1er juil. 2024 (RO **2024** 224).

2 La certification de sécurité est effectuée par le service spécialisé de la Confédération pour la sécurité de l'information, après consultation du service cryptographique de l'armée et d'armasuisse.[13]

3 Elle atteste que le moyen informatique remplit les exigences minimales correspondant à l'échelon de classification concerné et que les risques résiduels sont acceptables en fonction de l'état des connaissances techniques.

4 Elle est répétée en cas de changements importants concernant les risques ou le moyen informatique.

5 Le Département fédéral de la défense, de la protection de la population et des sports (DDPS) fixe la procédure relative à la certification de sécurité en tenant compte des normes internationales en la matière.

Art. 24 Protection en cas de menace pour des informations classifiées
(art. 10, al. 1, et 11, al. 1, LSI)

1 Quiconque constate que des informations classifiées ont été compromises, ont disparu ou qu'il en a été fait une utilisation abusive ou encore que des informations n'ont pas été classifiées alors qu'elles auraient dû l'être ou qu'elles ont été classifiées de manière erronée prend les mesures de protection nécessaires.

2 Il en informe immédiatement l'auteur de la classification et les organes de sécurité concernés.

Art. 25 Contrôle du besoin de protection et cercle des personnes autorisées
(art. 11, al. 2, LSI)

Les auteurs de la classification contrôlent le besoin de protection de leurs informations classifiées et le cercle des personnes autorisées au moins tous les cinq ans et les examinent systématiquement lorsque les informations sont proposées aux Archives fédérales.

Art. 26 Archivage
(art. 12, al. 3, LSI)

1 L'archivage des informations classifiées est régi par les dispositions de la législation fédérale sur l'archivage.

2 Les Archives fédérales veillent à ce que la sécurité de l'information visée dans la présente ordonnance soit garantie.

3 Les archives cessent d'être classifiées une fois que le délai de protection est échu. La prolongation du délai de protection est régie par l'art. 14 de l'ordonnance du 8 septembre 1999 sur l'archivage[14].

13 Nouvelle teneur selon l'art. 44 al. 2 ch. 1 de l'O du 1er mai 2024 sur l'organisation des marchés publics de l'administration fédérale, en vigueur depuis le 1er juil. 2024 (RO **2024** 224).
14 RS **152.11**

Section 5 Sécurité des moyens informatiques

Art. 27 Procédure de sécurité
(art. 16 LSI)

1 Les unités administratives visées à l'art. 2, al. 1, let. c, doivent pouvoir démontrer le besoin de protection de leurs objets à protéger et leur importance pour la gestion de la continuité des activités.

2 Elles mettent en œuvre les consignes minimales des différentes catégories de sécurité et vérifient si des mesures de sécurité supplémentaires sont nécessaires.

3 Elles démontrent les risques résiduels.

4 Les responsables de la sécurité de l'information (art. 36) décident si les risques résiduels sont acceptables. Ils peuvent déléguer cette décision à d'autres membres de la direction.

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

6 Les unités administratives visées à l'art. 2, al. 1, let. c, contrôlent chaque année si un changement important a eu lieu.

7 Le service spécialisé de la Confédération pour la sécurité de l'information émet des directives générales et abstraites s'appliquant à toutes les organisations visées à l'art. 2, al. 1 à 3, qui concernent la procédure de sécurité visée à l'art. 16 LSI.

Art. 28 Attribution des catégories de sécurité «protection élevée» et «protection très élevée»
(art. 17 LSI)

1 La catégorie de sécurité «protection élevée» est attribuée à un moyen informatique lorsqu'une violation de la sécurité de l'information est susceptible de provoquer un préjudice visé à l'art. 19 ou un dommage de 50 à 500 millions de francs.

2 La catégorie de sécurité «protection très élevée» est attribuée à un moyen informatique lorsqu'une violation de la sécurité de l'information est susceptible de provoquer un préjudice visé à l'art. 20 ou un dommage supérieur à 500 millions de francs.

Art. 29 Mesures de sécurité
(art. 6, al. 3, 18 et 85 LSI)

1 Le service spécialisé de la Confédération pour la sécurité de l'information émet des directives générales et abstraites s'appliquant à toutes les organisations visées à l'art. 2, al. 1 à 3, qui concernent les exigences minimales pour les catégories de sécurité visées à l'art. 17 LSI.

2 Il tient compte des exigences concernant la sécurité des données personnelles au sens de la législation sur la protection des données et celle des autres informations que la Confédération doit protéger en vertu de ses obligations légales ou contractuelles.

3 L'efficacité des mesures de sécurité applicables aux moyens informatiques suivants doit être contrôlée avant leur mise en exploitation, ainsi que durant l'exploitation en cas de changements importants des risques, mais au moins tous les cinq ans:

a. les moyens informatiques de la catégorie de sécurité «protection élevée» qui sont utilisés pour accomplir des tâches dépassant le cadre d'une autorité ou d'un département;

b. les moyens informatiques de la catégorie de sécurité «protection très élevée».

4 La ChF et les départements intègrent leurs moyens informatiques de la catégorie de sécurité «protection très élevée» dans leur gestion de la continuité.

Art. 30 Sécurité de l'exploitation
(art. 19 LSI)

1 Les unités administratives visées à l'art. 2, al. 1, let. c, veillent à ce que les responsabilités en matière de sécurité de l'information au niveau opérationnel soient consignées dans les accords de projets et les conventions de prestations conclus avec les fournisseurs internes de prestations.

2 Les fournisseurs internes de prestations mettent à la disposition des unités administratives visées à l'art. 2, al. 1, let. c, des départements et du service spécialisé de la Confédération pour la sécurité de l'information les informations dont ceux-ci ont besoin pour assurer la sécurité de l'information.

3 Ils veillent à disposer, sur le plan du personnel et des finances, des capacités et compétences nécessaires à la détection précoce, à l'analyse technique et à la maîtrise ou au traitement des incidents et des failles de sécurité qui les concernent ou qui concernent les bénéficiaires de leurs prestations dans le cadre des accords et conventions visés à l'al. 1.

4 Ils surveillent l'utilisation de leur infrastructure informatique et l'examinent régulièrement à la recherche de menaces et de vulnérabilités techniques. Ils peuvent charger des tiers d'effectuer cet examen.

5 Le traitement des données personnelles dans le cadre de la surveillance et de l'examen visés à l'al. 4 est régi par l'ordonnance du 22 février 2012 sur le traitement des données personnelles et des données des personnes morales lors de l'utilisation de l'infrastructure électronique de la Confédération[15].

Section 6 Mesures relatives aux personnes et protection physique

Art. 31 Vérification de l'identité des personnes et des machines
(art. 20 et 85 LSI)

1 Après avoir consulté le délégué TNI, le service spécialisé de la Confédération pour la sécurité de l'information peut émettre des directives générales et abstraites s'appliquant à toutes les organisations visées à l'art. 2, al. 1 à 3, qui concernent les

15 RS **172.010.442**

exigences techniques minimales auxquelles doit satisfaire la vérification, en fonction du risque, de l'identité des personnes et des machines qui ont besoin d'accéder à des informations, à des moyens informatiques, à des locaux et à d'autres infrastructures de la Confédération.

2 Le traitement des données personnelles effectué lors de la vérification de l'identité dans les systèmes de gestion des données d'identification visés à l'art. 24 LSI est régi par les dispositions de l'ordonnance du 19 octobre 2016 sur les systèmes de gestion des données d'identification et les services d'annuaires de la Confédération[16].

Art. 32 Sécurité relative aux personnes
(art. 6, al. 2 et 3, 8 et 20, al. 1, let. a et c, LSI)

1 Les unités administratives visées à l'art. 2, al. 1, let. c, veillent à ce que les collaborateurs soumis à un contrôle de sécurité relatif aux personnes visé dans l'ordonnance du 8 novembre 2023 sur les contrôles de sécurité relatifs aux personnes (OCSP)[17] soient sensibilisés chaque année à l'activité sensible déterminante et aux risques qui y sont liés.

2 Ces collaborateurs sont tenus d'annoncer à leur employeur les circonstances privées ou professionnelles susceptibles de les empêcher d'exercer leur activité sensible dans le respect des prescriptions.

Art. 33 Soupçon de comportement répréhensible
(art. 7, al. 2, let. c, LSI)

1 Lorsque la violation des prescriptions en matière de sécurité de l'information paraît constituer en même temps une infraction, la ChF et les départements transmettent le dossier de l'enquête et les procès-verbaux d'audition au Ministère public de la Confédération ou à l'auditeur en chef de l'armée suisse.

2 Ils saisissent les objets qui sont à même de servir de moyens de preuve dans une procédure.

Art. 34 Mesures de protection physique
(art. 22 et 85 LSI)

1 Après avoir consulté les organes de l'administration fédérale et de l'armée responsables de la sécurité des objets, le service spécialisé de la Confédération pour la sécurité de l'information peut émettre des directives générales et abstraites s'appliquant à toutes les organisations visées à l'art. 2, al. 1 à 3, qui concernent les exigences minimales de protection physique des informations et des moyens informatiques.

2 Il tient compte à cet égard:

a. du cycle de vie entier des informations et des moyens informatiques;

b. des exigences spécifiques à la place de travail;

16 RS **172.010.59**
17 RS **128.31**

c. des stratégies et des plans d'hébergement de l'administration fédérale et de l'armée.

Art. 35 Zones de sécurité
(art. 23 et 85 LSI)

[1] Les unités administratives visées à l'art. 2, al. 1, let. c, peuvent établir les zones de sécurité suivantes:

a. zone de sécurité 1: les locaux et les espaces dans lesquels des informations classifiées «confidentiel» sont fréquemment traitées ou des moyens informatiques de la catégorie de sécurité «protection élevée» sont exploités;

b. zone de sécurité 2: les locaux et les espaces dans lesquels des informations classifiées «secret» sont fréquemment traitées ou des moyens informatiques de la catégorie de sécurité «protection très élevée» sont exploités.

[2] Ces locaux et ces espaces ne sont considérés comme des zones de sécurité que si l'organe de l'administration fédérale ou de l'armée responsable de la sécurité des objets confirme avant leur mise en exploitation et ensuite au moins tous les cinq ans que les exigences en matière de sécurité sont remplies.

[3] Après avoir consulté les organes de l'administration fédérale et de l'armée responsables de la sécurité des objets, le service spécialisé de la Confédération pour la sécurité de l'information émet des directives générales et abstraites s'appliquant à toutes les organisations visées à l'art. 2, al. 1 à 3, qui concernent les exigences en matière de sécurité pour les zones de sécurité et leur établissement.

[4] Les unités administratives visées à l'art. 2, al. 1, let. c, peuvent prendre des mesures aux alentours des zones de sécurité afin d'identifier les actes d'espionnage électromagnétique et de s'en protéger.

Section 7 Organisation de sécurité

Art. 36 Responsables de la sécurité de l'information des unités administratives visées à l'art. 2, al. 1, let. c
(art. 7, al. 1, LSI)

[1] Le chancelier de la Confédération, les secrétaires généraux et les directeurs des unités administratives visées à l'art. 2, al. 1, let. c, sont responsables de la sécurité de l'information dans leur domaine de compétence.

[2] Ils peuvent déléguer la responsabilité en matière de sécurité de l'information à un membre de la direction s'il dispose des pouvoirs nécessaires pour prendre des mesures, les contrôler et les corriger.

[3] Les responsables de la sécurité de l'information des unités administratives visées à l'art. 2, al. 1, let. c, assument notamment les tâches suivantes:

a. ils assurent la mise en place, l'exploitation, le contrôle et l'amélioration continue du SMSI dans leur domaine de compétence et émettent les directives nécessaires;

b. ils prennent toutes les décisions qui ont une influence déterminante sur la sécurité de l'information dans leur domaine de compétence, notamment concernant l'organisation, les processus, l'acceptation des risques et les objectifs de sécurité;

c. ils décident des mesures nécessaires, notamment concernant la formation et la sensibilisation;

d. ils approuvent la planification annuelle de contrôle et d'audit et mettent les ressources nécessaires à disposition.

4 Le chancelier de la Confédération, les secrétaires généraux et les directeurs des unités administratives visées à l'art. 2, al. 1, let. c, confient des tâches à leurs préposés à la sécurité de l'information visés à l'art. 37 et s'assurent:

a. qu'ils disposent des compétences et des ressources appropriées, et

b. qu'ils ne se voient confier aucune tâche susceptible d'entraîner un conflit d'intérêts avec les tâches visées à l'art. 37.

Art. 37 Préposés à la sécurité de l'information des unités administratives visées à l'art. 2, al. 1, let. c
(art. 7, al. 1, LSI)

1 Les unités administratives visées à l'art. 2, al. 1, let. c, désignent un ou plusieurs préposés à la sécurité de l'information et leurs suppléants.

2 Les préposés à la sécurité de l'information accomplissent les tâches et assument les compétences suivantes:

a. ils exploitent le SMSI de l'unité administrative sur mandat du responsable de la sécurité de l'information;

b. ils élaborent les bases de décision nécessaires à l'intention du responsable de la sécurité de l'information et lui proposent des mesures à prendre;

c. ils sont les interlocuteurs principaux de l'unité administrative pour les questions de sécurité de l'information et conseillent les personnes et les services responsables et les aident à accomplir leurs tâches et à exécuter leurs obligations dans le domaine de la sécurité de l'information;

d. ils veillent à la mise en œuvre des directives en matière de sécurité de l'information et à l'application de la procédure de sécurité visée à l'art. 27;

e. ils exercent la surveillance de la liste des bases légales, de l'inventaire des objets à protéger et de la liste des autorisations exceptionnelles;

f. ils exercent la surveillance de la planification de la formation et de la sensibilisation visées à l'art. 11 et proposent au responsable de la sécurité de l'information l'organisation de mesures de formation et de sensibilisation supplémentaires;

g. ils demandent l'ouverture de la procédure de sécurité relative aux entreprises visée à l'art. 4 de l'ordonnance du 8 novembre 2023 sur la procédure de sécurité relative aux entreprises (OPSEnt)[18];

h. ils coordonnent la maîtrise des incidents de sécurité et le traitement des failles de sécurité dans l'unité administrative et auprès des tiers mandatés;

i. ils établissent la planification annuelle de contrôle et d'audit et la soumettent au responsable de la sécurité de l'information pour approbation;

j. ils contrôlent périodiquement la présence de supports d'information classifiés «secret» et la sécurité de ceux-ci dans leur domaine de compétence;

k. sur mandat du responsable de la sécurité de l'information, ils peuvent contrôler ou faire contrôler l'utilisation des informations aux postes de travail ouverts, partagés ou non verrouillables et dans les moyens informatiques de l'unité administrative;

l. ils rendent compte chaque semestre au responsable de la sécurité de l'information de la situation en matière de sécurité de l'information.

Art. 38[19] Sécurité de l'information dans les moyens informatiques mis à disposition de manière centralisée

1 Le délégué TNI est chargé de garantir la sécurité de l'information dans les moyens informatiques mis à disposition de manière centralisée par le secteur TNI.

2 Il désigne un ou plusieurs préposés à la sécurité de l'information et leurs suppléants.

3 Les préposés à la sécurité de l'information assument les tâches visées à l'art. 37, al. 2, pour les moyens informatiques mis à disposition de manière centralisée par le secteur TNI et informent l'administration fédérale et l'armée des risques pour la sécurité de l'information.

Art. 39 Responsabilité des départements en matière de sécurité de l'information
(art. 7, al. 1, et 81 LSI)

1 Les départements sont responsables du pilotage et de la surveillance de la sécurité de l'information dans leur domaine de compétence.

2 Ils accomplissent à cet égard notamment les tâches suivantes:

a. ils déterminent la politique en matière de sécurité de l'information et l'organisation de sécurité du département, y compris la conduite technique des préposés à la sécurité de l'information visés à l'art. 37;

b. ils édictent les directives nécessaires et en surveillent la mise en œuvre;

c. ils surveillent le SMSI des unités administratives visées à l'art. 2, al. 1, let. c, et relèvent les indicateurs nécessaires à cette fin;

18 RS **128.41**
19 Nouvelle teneur selon l'annexe 2 ch. II 1 de l'O du 2 avr. 2025 sur la numérisation, en vigueur depuis le 1er mai 2025 (RO **2025** 235).

d. ils fixent des objectifs annuels de sécurité pour les unités administratives visées à l'art. 2, al. 1, let. c, et vérifient qu'elles les ont atteints;

e. ils approuvent la planification annuelle de contrôle et d'audit du département et mettent les ressources nécessaires à disposition;

f. ils confient des tâches à leurs préposés à la sécurité de l'information visés à l'art. 40 et s'assurent:

1. qu'ils disposent des compétences et des ressources appropriées, et
2. qu'ils ne se voient confier aucune tâche susceptible d'entraîner un conflit d'intérêts avec les tâches visées à l'art. 40.

3 Ils peuvent fixer pour leur domaine de compétence des exigences en matière de sécurité qui dépassent les exigences minimales du service spécialisé de la Confédération pour la sécurité de l'information.

4 Pour autant que le chef de département n'en décide pas autrement, la sécurité de l'information dans le département relève de la responsabilité du secrétaire général qui agit sous son mandat.

Art. 40 Préposés à la sécurité de l'information des départements
(art. 7, al. 1, et 81 LSI)

Les préposés à la sécurité de l'information des départements accomplissent les tâches suivantes en plus de celles qui sont visées à l'art. 81, al. 2, LSI:

a. ils assurent la coordination interdépartementale de la sécurité de l'information;

b. ils élaborent les bases de décision nécessaires à l'intention du responsable de la sécurité de l'information et lui proposent des mesures à prendre;

c. ils coordonnent la maîtrise des incidents de sécurité et le traitement des failles de sécurité impliquant plusieurs unités administratives visées à l'art. 2, al. 1, let. c;

d. ils établissent la planification annuelle de contrôle et d'audit du département et la soumettent au responsable de la sécurité de l'information pour approbation;

e. ils représentent le département au sein d'organes spécialisés;

f. ils sont consultés pour le choix des préposés à la sécurité de l'information des unités administratives visés à l'art. 37;

g. ils vérifient périodiquement et en cas de changement ou de départ d'un membre du Conseil fédéral ou du chancelier de la Confédération que tous les supports d'information classifiés «secret» sont présents et au complet;

h. ils rendent compte chaque année au responsable de la sécurité de l'information du département de la situation en matière de sécurité de l'information dans le département.

Art. 41 Préposé à la sécurité de l'information du Conseil fédéral
(art. 81, al. 1, let. a, LSI)

Le DDPS nomme le préposé à la sécurité de l'information du Conseil fédéral et son suppléant.

Art. 42 Service spécialisé de la Confédération pour la sécurité de l'information
(art. 7, al. 1, et 83 LSI)

1 Le service spécialisé de la Confédération pour la sécurité de l'information accomplit les tâches et assume les compétences suivantes pour l'administration fédérale et l'armée:

a. il élabore des stratégies sur des thèmes pertinents pour la sécurité;

b. il peut demander des informations, émettre des avis et proposer des modifications concernant des projets dans le domaine de la sécurité;

c. il participe à la formation des membres de l'organisation de sécurité;

d. il prépare des modèles et des aides;

e. il aide les préposés à la sécurité de l'information à contrôler les supports d'information classifiés «secret»;

f. il assume la responsabilité des solutions de sécurité certifiées utilisées dans toute l'administration fédérale et l'armée.

2 Il consulte la Conférence des préposés à la sécurité de l'information lors de l'accomplissement de ces tâches et de celles visées à l'art. 83, al. 1, LSI.

3 Il représente la Suisse dans les relations internationales en tant qu'autorité nationale de sécurité et assume dans ce contexte les tâches suivantes:

a. il élabore les traités internationaux visés à l'art. 87 LSI et en contrôle la mise en œuvre;

b. il veille à ce que les incidents de sécurité qui concernent des informations classifiées d'États partenaires soient clarifiés de manière appropriée;

c. il exécute les contrôles prévus dans les traités internationaux ou les fait exécuter;

d. il représente la Suisse dans des organismes internationaux spécialisés;

e. il autorise l'arrivée d'étrangers en Suisse pour participer à des projets classifiés et l'envoi de personnes à l'étranger pour participer à des projets classifiés;

f. il délivre les certificats de sécurité visés à l'art. 30 OCSP[20].

4 Il fait partie du Secrétariat d'État à la politique de sécurité du DDPS.

20 RS **128.31**

Art. 43 Tâches et compétences de l'OFCS
(art. 7, al. 1, et 84, al. 1, LSI)

1 L'OFCS accomplit les tâches et assume les compétences suivantes:

a. il conseille l'administration fédérale et l'armée ainsi que les organes de sécurité visés aux art. 81 à 83 LSI pour toutes les questions liées à la sécurité technique de l'information;

b. il siège à la Conférence des préposés à la sécurité de l'information visée à l'art. 82 LSI;

c. il peut, afin d'évaluer et d'améliorer la situation en matière de sécurité technique de l'information de la Confédération, rechercher des menaces et des vulnérabilités techniques sur Internet ou, en concertation avec les responsables de la sécurité de l'information et les fournisseurs de prestations, dans l'infrastructure informatique de l'administration fédérale; il peut en charger d'autres services de l'administration fédérale ou des tiers.

2 Il coordonne ses activités avec celles du service spécialisé de la Confédération pour la sécurité de l'information.

Section 8 Coûts et évaluation

Art. 44 Coûts

1 Les coûts décentralisés de la sécurité de l'information font partie des coûts de projet et d'exploitation.

2 Les unités administratives visées à l'art. 2, al. 1, let. c, veillent à ce que les coûts soient suffisamment pris en compte et démontrés lors de la planification.

3 Le service spécialisé de la Confédération pour la sécurité de l'information perçoit un émolument de 100 francs pour établir et envoyer les certificats de sécurité visés à art. 30 OCSP[21] pour les personnes qui n'exercent pas d'activité sensible de la Confédération.

Art. 45 Évaluation
(art. 88 LSI)

Six ans après l'entrée en vigueur de la présente ordonnance et ensuite tous les dix ans, le service spécialisé de la Confédération pour la sécurité de l'information demande au Contrôle fédéral des finances d'évaluer la législation sur la sécurité de l'information au sein de la Confédération.

21 RS **128.31**

Section 9 Traitement des informations et des données personnelles

Art. 46 Généralités

1 Les organisations visées à l'art. 2, al. 1 à 3, et les organes de sécurité de la Confédération peuvent traiter les informations utiles à la sécurité de l'information, y compris les données personnelles.

2 Ils peuvent échanger les informations, y compris les données personnelles, visées à l'al. 1 entre eux et avec des organisations nationales, internationales ou étrangères de droit public ou privé, dans la mesure où:

a. cela est utile à la sécurité de l'information;

b. aucune obligation de maintien du secret légale ou contractuelle n'est violée;

c. les dispositions de la législation fédérale en matière de protection des données sont respectées, et

d. ces organisations assument des tâches légales dans le domaine de la sécurité de l'information qui correspondent à celles de l'autorité ou de l'organisation qui communique les informations.

3 Pour autant que cela soit nécessaire pour maîtriser un incident de sécurité ou traiter une faille de sécurité, ils peuvent également traiter et échanger des données sensibles visées à l'art. 5, let. c, de la loi fédérale du 25 septembre 2020 sur la protection des données[22] de personnes qui ont ou auraient participé à l'incident ou à la faille de sécurité ou qui sont ou seraient concernées par l'incident ou la faille de sécurité.

4 Si, lors d'un incident de sécurité survenant au sein de la Confédération ou auprès de tiers collaborant avec la Confédération, des informations de la Confédération sont dérobées et publiées sur Internet, ils peuvent télécharger et analyser ces informations afin d'évaluer l'atteinte portée à la Confédération et de prendre les mesures de protection nécessaires. Ils ne peuvent pas traiter les données qui ne sont pas utiles à cette évaluation.

5 Ils peuvent appliquer ces mesures en cas de soupçon concret.

Art. 47 Application SMSI

1 Les organisations visées à l'art. 2, al. 1 à 3, peuvent exploiter un système d'information pour gérer la sécurité de l'information (application SMSI).

2 Elles peuvent traiter dans l'application SMSI toutes les informations liées à la gestion de la sécurité de l'information en vertu de la présente ordonnance et les données sensibles visées à l'art. 46, al. 3.

3 Elles peuvent relier leurs applications SMSI et échanger des informations pertinentes pour la sécurité de l'information par des interfaces automatisées.

22 RS **235.1**

Art. 48 Services électroniques de formulaire

[1] Le service spécialisé de la Confédération pour la sécurité de l'information peut exploiter des services électroniques de formulaire et les relier à son application SMSI dans les buts suivants:

a. gérer les déplacements visés à l'art. 42, al. 3, let. e;

b. établir et envoyer les certificats internationaux de sécurité visés à l'art. 30 OCSP[23];

c. établir et envoyer les certificats internationaux de sécurité visés à l'art. 66 LSI.

[2] Les données personnelles figurant dans l'annexe 1 peuvent être traitées à l'aide des services de formulaire visés à l'al. 1. Elles peuvent être conservées pendant dix ans au plus.

[3] Les organisations visées à l'art. 2, al. 1 à 3, peuvent exploiter des services électroniques de formulaire pour annoncer des incidents et des failles de sécurité et les relier à leur application SMSI.

[4] À l'aide des services de formulaire visés à l'al. 3, elles peuvent traiter les données personnelles, y compris les données sensibles visées à l'art. 46, al. 3, qui sont nécessaires à la maîtrise des incidents de sécurité et au traitement des failles de sécurité. Elles doivent effacer ces données du service de formulaire immédiatement après leur communication. Elles peuvent provisoirement les enregistrer avant l'envoi durant 24 heures au plus.

Section 10 Dispositions finales

Art. 49 Dispositions d'exécution particulières

Le DDPS peut déclarer contraignantes pour les cantons des versions datées des directives générales et abstraites visées aux art. 17, al. 3, 21, al. 1, 29, al. 1 et 34, al. 1.

Art. 50 Abrogation et modification d'autres actes

L'abrogation et la modification d'autres actes sont réglées dans l'annexe 2.

Art. 51 Dispositions transitoires

[1] Les directives en matière de sécurité informatique émises par le Centre national pour la cybersécurité (NCSC) et les exceptions qu'il a autorisées avant l'entrée en vigueur de la présente ordonnance conservent leur validité durant trois ans au plus après l'entrée en vigueur de la présente ordonnance.

[2] Le service spécialisé de la Confédération pour la sécurité de l'information ou le NCSC prend les décisions concernant les changements des directives et des exceptions autorisées émises par le NCSC avant l'entrée en vigueur de la présente ordonnance.

23 RS **128.31**

3 Les directives en matière de protection de l'information émises par la Conférence des secrétaires généraux ou l'organe de coordination pour la protection des informations au sein de la Confédération avant l'entrée en vigueur de la présente ordonnance conservent leur validité durant deux ans au plus après l'entrée en vigueur de la présente ordonnance.

4 Les unités administratives visées à l'art. 2, al. 1, let. c, mettent en place leur SMSI (art. 5) dans les trois ans après l'entrée en vigueur de la présente ordonnance.

5 Les catalogues de classification (art. 17) doivent être établis au plus tard un an après l'entrée en vigueur de la présente ordonnance.

6 L'OFCS assume jusqu'au 30 juin 2025 les tâches et les compétences du service spécialisé de la Confédération pour la sécurité de l'information visées aux art. 9, al. 2 et 3, 11, al. 3 et 4, 12, al. 3 et 6 à 8, 15, 27, al. 7, 29, al. 1, et 31, al. 1.

7 Les directives émises par l'OFCS en application de l'al. 6 conservent leur validité durant deux ans au plus après l'entrée en vigueur de la présente ordonnance.

Art. 52 Entrée en vigueur

La présente ordonnance entre en vigueur le 1er janvier 2024.

Annexe 1
(art. 48)

Traitement des données à l'aide de services électroniques de formulaire

Les données personnelles suivantes peuvent être traitées à l'aide des services de formulaire ci-dessous:

1. Service de formulaire pour le but visé à l'art. 48, al. 1, let. a

a. Données relatives à la personne:
   1. Prénoms et noms*
   2. Numéro AVS
   3. Civilité, titre et rang*
   4. Date de naissance*
   5. Lieu d'origine et lieu de naissance*
   6. Nationalités*
   7. Numéro de carte d'identité et de passeport, lieu d'établissement et validité*

b. Données concernant les fonctions professionnelles ou militaires de la personne:
   1. Fonction au sein de l'organisation ou de l'armée*
   2. Adresse professionnelle, adresse e-mail, numéros de téléphone et autres coordonnées, en particulier électroniques
   3. Décision positive concernant le contrôle de sécurité relatif aux personnes, degré de contrôle et durée de validité*

c. Données relatives à l'organisation requérante:
   1. Nom, adresse et coordonnées de l'organisation*
   2. Prénoms et noms de la personne de référence
   3. Fonction de la personne de référence au sein de l'organisation ou de l'armée
   4. Adresse professionnelle, adresse e-mail, numéros de téléphone et coordonnées électroniques de la personne de référence

d. Données concernant la visite:
   1. Nom, adresse, adresse e-mail et coordonnées de l'organisation étrangère*
   2. Motif de la visite*
   3. Catégorie de sécurité de la visite*
   4. Durée de la visite*
   5. Points du passage de la frontière*

6. Moyens de transport*
7. Matériel transporté, y c. armes, munitions, explosifs, véhicules et autres équipements*

Les données suivies d'un astérisque (*) sont communiquées à l'autorité de sécurité étrangère.

2. Service de formulaire pour le but visé à l'art. 48, al. 1, let. b

a. Données relatives à la personne:
   1. Prénoms et noms
   2. Numéro AVS
   3. Civilité, titre et rang
   4. Date de naissance
   5. Lieu d'origine et lieu de naissance
   6. Nationalités
   7. Numéro de carte d'identité et de passeport, lieu d'établissement et validité

b. Données concernant les fonctions professionnelles ou militaires de la personne:
   1. Fonction au sein de l'organisation ou de l'armée
   2. Adresse professionnelle, adresse e-mail, numéros de téléphone et autres coordonnées, en particulier électroniques
   3. Décision positive concernant le contrôle de sécurité relatif aux personnes, degré de contrôle et durée de validité

c. Données relatives à l'organisation requérante:
   1. Nom, adresse, adresse e-mail et coordonnées de l'organisation
   2. Prénoms et noms de la personne de référence
   3. Fonction de la personne de référence au sein de l'organisation ou de l'armée
   4. Adresse professionnelle, adresse e-mail et autres coordonnées, en particulier électroniques, de la personne de référence
   5. Motif de l'établissement du certificat

3. Service de formulaire pour le but visé à l'art. 48, al. 1, let. c

a. Données relatives à l'entreprise:
   1. Nom complet*
   2. Forme juridique*
   3. Numéro d'identification de l'entreprise
   4. Adresse, adresse e-mail et autres coordonnées, en particulier électroniques*
   5. Siège*
   6. Prénoms et noms de la personne de référence*

7. Fonction de la personne de référence au sein de l'entreprise
8. Adresse professionnelle, adresse e-mail et autres coordonnées, en particulier électroniques, de la personne de référence

b. Données concernant la déclaration de sécurité relative aux entreprises:
   1. Date d'établissement et durée de validité*
   2. Champ d'application et charges*
   3. Échelon de classification ou catégorie de sécurité le plus élevé autorisé*

Les données suivies d'un astérisque (*) sont communiquées à l'autorité de sécurité étrangère.

4. Service de formulaire visé à l'art. 48, al. 3

a. Données concernant l'auteur de l'annonce:
   1. Prénoms et noms
   2. Adresse, adresse e-mail, numéros de téléphone et autres coordonnées, en particulier électroniques
   3. Fonction au sein de l'organisation ou de l'armée

b. Données relatives au dommage et au calcul du dommage

c. Photographies, enregistrements sonores ou vidéos de l'incident ou de la faille de sécurité

d. Documents ou fichiers portant sur l'incident ou la faille de sécurité

e. Données relatives aux éventuelles personnes impliquées dans l'incident

f. Premières analyses de spécialistes, y compris premières mesures prises

Annexe 2
(art. 50)

Abrogation et modification d'autres actes

I

L'ordonnance du 27 mai 2020 sur les cyberrisques[24] est abrogée.

II

Les actes mentionnés ci-après sont modifiés comme suit:

…[25]

24 [RO **2020** 2107, 5871 annexe ch. 1; **2021** 132]
25 Les mod. peuvent être consultées au RO **2023** 735.