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

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

du … Avant-projet du 24 août 2022

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, 3 et 84, al. 3, LSI)

[1] La présente ordonnance s'applique:

a. au Conseil fédéral;

b. aux unités de l'administration fédérale centrale au sens de l'art. 7 de l'ordonnance du 25 novembre 1998 sur l'organisation du gouvernement et de l'administration (OLOGA)[2];

c. à l'armée.

[2] La LSI et la présente ordonnance s'appliquent aux unités de l'administration fédérale décentralisée au sens de l'art. 7*a* OLOGA[3] de la manière suivante:

RS **128.1**

1 RS **128**
2 RS **172.010.1**
3 RS **172.010**

a. aux unités administratives qui ont accès aux moyens informatiques des fournisseurs internes de prestations informatiques visés à l'art. 9 de l'ordonnance du 25 novembre 2020 sur la transformation numérique et l'informatique (OTNI)[4] relevant des catégories de sécurité «protection élevée» ou «protection très élevée» visées à l'art. 28: la LSI et la présente ordonnance;

b. aux unités administratives qui utilisent les moyens informatiques relevant des catégories de sécurité «protection élevée» ou «protection très élevée» visées à l'art. 28: la LSI et la présente ordonnance;

c. aux unités administratives qui ne sont pas concernées par les let. a et b, mais qui traitent des informations classifiées de la Confédération: les art. 9 à 15 et 27 à 73 LSI et les dispositions de la section 4 de la présente ordonnance.

3 La Chancellerie fédérale ou les départements peuvent demander au Conseil fédéral de soumettre à la LSI, à la présente ordonnance ou à certaines des parties de cette dernière les unités administratives de l'administration fédérale décentralisée qui ne sont pas concernées par l'al. 2.

4 L'annexe 1 porte sur:

a. les unités administratives visées à l'al. 2;

b. les unités administratives visées à l'al. 3 et les dispositions de la LSI et de la présente ordonnance qui les concernent.

5 Les organisations visées à l'art. 2, al. 4, de la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA)[3] sont exclues du champ d'application de la LSI et de la présente ordonnance.

6 S'appliquent aux cantons sous réserve de l'art. 3, al. 2, LSI:

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

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

Section 2 Principes

Art. 3 Objectifs de sécurité

(art. 7, al. 2, let. a, LSI)

1 Les organisations visées à l'art. 2 veillent ensemble à protéger leurs informations et leurs moyens informatiques en fonction des risques et à faire preuve d'une résilience appropriée envers les risques pour la sécurité de l'information.

2 En collaborant et en échangeant des informations avec les autres autorités fédérales, les cantons, les communes, l'économie, la société, les milieux scientifiques et les partenaires internationaux, elles contribuent à améliorer durablement la sécurité de l'information de la Suisse.

4 RS **172.010.58**

3 Elles s'engagent à harmoniser sur le plan national et international les prescriptions et les niveaux en matière de sécurité afin de permettre l'interaction des autorités fédérales avec d'autres autorités de la Confédération, des cantons et des communes.

Art. 4 Responsabilité

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

2 Elles assument toutes les tâches qui relèvent de leur domaine de compétence que la présente ordonnance et le 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 ou utilisent des informations ou des moyens informatiques de la Confédération sont responsables du respect des prescriptions en la matière.

4 Les supérieurs hiérarchiques de tous les échelons sont responsables de la formation de leurs collaborateurs dans le domaine de la sécurité de l'information en fonction de leurs tâches et s'assurent que leurs collaborateurs respectent les directives.

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 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 le département et veillent à continuellement améliorer 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 engagements contractuels
(art. 7, al. 1, LSI)

1 Les unités administratives, 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.

2 Les unités administratives et les départements consultent le service spécialisé de la Confédération pour la sécurité de l'information en cas de directives et de projets dans le domaine de la sécurité.

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

1 Les unités administratives dressent l'inventaire de leurs objets à protéger et le tiennent un jour.

2 Par objets à protéger, on entend:

a. les collections de toutes les données traitées dans le but d'exécuter une tâche de la Confédération;

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

3 L'inventaire sert à justifier:

a. le besoin de protection des objets à protéger;

b. les responsabilités liées aux objets à protéger;

c. le cas échéant. l'utilisation partagée de l'objet à protéger;

d. la participation de tiers;

e. le résultat de l'évaluation des risques;

f. la mise en œuvre des mesures de sécurité et l'acceptation des risques résiduels;

g. les contrôles et les audits périodiques.

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

1 Les unités administratives évaluent en continu les risques pour leurs objets à protéger et assument pour ce faire 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, les unités administratives qui fournissent des prestations et les organes de sécurité de la Confédération informent les unités administratives et les départements des menaces et vulnérabilités actuelles et des risques qui les concernent. Ils émettent au besoin des recommandations de mesures de limitation des risques.

3 Les unités administratives 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 exceptions
(art. 7, al. 1, LSI)

1 Si une unité administrative n'est pas en mesure d'observer une directive concernant un objet à protéger, elle a besoin d'une autorisation du service ayant émis la directive.

2 Le service spécialisé de la Confédération pour la sécurité de l'information et les départements peuvent déléguer l'octroi d'exceptions.

3 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 Chancellerie fédérale sur la transition numérique et la gouvernance de l'informatique, le service spécialisé de la Confédération pour la sécurité de l'information consulte au préalable le délégué TNI conformément à l'art. 4, al. 1, OTNI[5].

4 Les unités administratives, les départements et le service spécialisé de la Confédération pour la sécurité de l'information tiennent à jour la liste des autorisations exceptionnelles:

a. qu'ils ont eux-mêmes accordées;

b. qui ont été accordées pour leurs propres objets à protéger.

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

1 Les unités administratives évaluent à la lumière les directives de l'art. 8 les risques encourus par leurs objets à protéger lors de la collaboration avec des tiers et leur dépendance envers des tiers.

2 Les services d'achat visés aux art. 9 et 10 de l'ordonnance du 24 octobre 2012 sur l'organisation des marchés publics de l'administration fédérale (Org-OMP)[6] collaborent à l'évaluation et mettent les informations nécessaires à disposition.

3 Après avoir consulté la Conférence des achats de la Confédération visée à l'art. 24 Org-OMP, le service spécialisé de la Confédération pour la sécurité de l'information émet des recommandations quant aux dispositions relatives à la sécurité de l'information que doivent contenir tous les contrats d'acquisition et de prestation de la Confédération.

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

1 Les unités administratives 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 tiennent la liste des formations et des participants.

2 La formation comprend notamment:

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

5 RS **172.010.58**
6 RS **172.056.15**

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 personnes de contact en cas de questions relatives à la sécurité de l'information;

e. les tâches de contrôle des supérieurs hiérarchiques;

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

3 Les unités administratives, 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 assure la coordination et 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 fixent en accord avec les fournisseurs de prestations la manière dont les incidents et les failles de sécurité sont annoncées et maîtrisées. Elles règlent également la compétence décisionnelle en matière de mesures urgentes.

2 Les fournisseurs de prestations annoncent immédiatement aux unités administratives auxquelles ils fournissent leurs prestations les incidents et les failles de sécurité qui les concernent et les aident à les maîtriser.

3 Le service spécialisé de la Confédération pour la sécurité de l'information peut aider les unités administratives et les départements à maîtriser les incidents de sécurité et à traiter les failles de sécurité.

4 Les unités administratives 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 ou de l'armée 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 selon 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 visée 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. Il a dans ce cadre les tâches et les compétences suivantes:

a. il peut obliger les unités administratives, les fournisseurs de prestations et les tiers à lui communiquer toutes les informations nécessaires;

b. il peut ordonner des mesures urgentes;

c. il peut demander l'aide de spécialistes externes;

d. il informe la direction de l'unité administrative concernée 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 rend la direction de la gestion 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 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 de 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 visé à l'art. 51, al. 2, LSI.

3 Le service spécialisé de la Confédération pour la sécurité de l'information collecte 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 et le communique 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 Les départements et la Chancellerie fédérale 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.

2 Ils collectent les informations nécessaires auprès des unités administratives et de leurs fournisseurs de prestations.

3 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.

4 Il fixe les modalités des comptes rendus des fournisseurs internes de prestations visés à l'art. 9 OTNI[7].

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

Art. 15 Directives de 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 tous les services visés à l'art. 2, al. 1 à 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 LSI)

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

2 Si des informations sont regroupées dans un recueil, il faut contrôler si celui-ci doit être classifié ou recevoir un échelon de classification supérieur.

3 En cas de demande d'accès à des documents officiels, l'instance compétente examine, indépendamment de l'éventuelle mention de classification, s'il y a lieu d'autoriser, de limiter, de différer ou de refuser l'accès conformément aux dispositions de la loi du 17 décembre 2004 sur la transparence[8].

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

1 Les personnes et les services suivants sont compétents pour classifier et déclassifier les informations:

a. le personnel de la Confédération et les militaires: les supports d'information qu'ils produisent ou font produire et les informations qu'ils communiquent oralement;

b. les collaborateurs d'entreprises disposant d'une déclaration de sécurité visée à l'art. 61 LSI: les supports d'information qu'ils produisent sur mandat de la Confédération;

7 RS **172.010.58**
9 RS **152.3**

c. la personne responsable de la tâche: les objets à protéger visés à l'art. 7, al. 2, let. a.

2 Les unités administratives, la Chancellerie fédérale et les départements fixent dans un catalogue de classification la manière de classifier les informations souvent traitées dans leur domaine de compétence.

3 Le service spécialisé de la Confédération pour la sécurité de l'information contrôle le catalogue de classification visé à l'al. 2 et émet si nécessaire une recommandation.

4 Il fixe, après avoir consulté la Conférence des préposés à la sécurité de l'information, dans un catalogue de classification la manière de classifier les informations souvent traitées dans l'administration fédérale et à l'armée.

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

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 important processus de conduite de l'armée est nettement 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 nettement 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 durant des mois.

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 ou la liberté 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 conforme d'opérations des autorités de poursuite pénale, du SRC, de l'armée ou des autres organes de sécurité de la Confédération est compromise;

c. les moyens et les méthodes opérationnelles des services de renseignement et des autorités de poursuite pénale de la Confédération ou l'identité des sources et des 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 interrompues;

h. la position de la Suisse est provisoirement 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 troupes l'armée est annihilée durant des jours ou entravée sérieusement 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. les 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 dans une mesure particulièrement importante durant plusieurs semaines 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 plusieurs 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 plusieurs 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 tous les services visés à l'art. 2, al. 1 à 3 qui concernent le traitement des informations classifiées et fixe les exigences de sécurité en matière d'organisation, de personnel et de construction, de même que sur le plan technique.

2 Il consulte au préalable les services suivants:

a. le service cryptographique de l'armée;

b. les services ayant la compétence d'acheter des biens cryptologiques visés à l'art. 10, al. 1, let. d, Org-OMP[9], et

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

3 Il tient compte des normes internationales.

4 La Chancellerie fédérale règle le traitement des affaires classifiées du Conseil fédéral.

5 Le traitement des informations classifiées provenant de l'étranger est régi par les prescriptions correspondant à l'échelon de classification étranger. Les prescriptions 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 d'utilisateurs fermé clairement identifiable, les personnes suivantes peuvent, après avoir consulté le service spécialisé de la Confédération pour la sécurité de l'information, fixer 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 de la sécurité des frontières.

2 Les personnes visées à l'al. 1 veillent à ce que l'on sache clairement si les prescriptions de traitement simplifié s'appliquent.

9 RS **172.056.15**

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

1 Les moyens informatiques doivent être accrédités avant leur mise en service sur le plan de la sécurité si l'une des conditions suivantes est remplie:

a. ils sont utilisés pour accomplir des tâches dépassant le cadre d'un office et impliquant le traitement d'informations classifiées «secret»;

b. ils sont utilisés pour accomplir des tâches dépassant le cadre d'une autorité ou d'un département et impliquant le traitement d'informations classifiées «confidentiel»;

c. l'accréditation de sécurité est nécessaire à la collaboration nationale et internationale.

2 L'accréditation de sécurité atteste que le moyen informatique remplit les exigences minimales de sécurité correspondant à l'échelon de classification concerné et que les risques résiduels sont supportables conformément à l'état des connaissances techniques.

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

4 Si l'accréditation de sécurité ne peut pas être octroyée parce que le moyen informatique ne remplit pas les exigences minimales de sécurité, le Conseil fédéral prend la décision concernant les risques résiduels.

5 Le service spécialisé de la Confédération pour la sécurité de l'information assume les tâches suivantes:

a. il octroie l'accréditation de sécurité après avoir entendu le service cryptographique de l'armée et les services visés à l'art. 10, al. 1, let. d, Org-OMP[10];

b. il peut déléguer au Groupement Défense la compétence d'accréditer uniquement les systèmes militaires.

6 Le [département compétent] fixe la procédure relative à l'accréditation de sécurité en tenant compte des normes internationales en la matière.

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

1 Celui qui constate que des informations classifiées ont été compromises, ont disparu ou qu'il en a été fait un usage abusif ou que des informations n'ont par erreur pas été classifiées ou qu'elles ont été classifiées de manière erronée prend les mesures de protection nécessaires.

10 RS **172.056.15**

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

Art. 25 Contrôle du besoin de protection et 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 l'examine 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 prescriptions 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 Il n'est plus nécessaire de classifier les archives une fois que le délai de protection est échu. Une prolongation du délai de protection est régie par l'art. 14 de l'ordonnance du 8 septembre 1999 sur l'archivage[11].

Section 5 Sécurité des moyens informatiques

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

1 Les unités administratives doivent pouvoir démontrer le besoin de protection de leurs objets à protéger et leur importance pour la gestion de la continuité relative à l'exploitation.

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

3 Elles démontrent les risques qui ne peuvent pas être réduits de manière suffisante (risques résiduels).

4 Les responsables de la sécurité visés à l'art. 36 décident si les risques résiduels sont jugés 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 et la situation de l'organisation.

6 Les unités administratives contrôlent chaque année si un changement important au sens de l'al. 5 a eu lieu.

11 RS **152.11**

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 considérable selon l'art. 19 ou un préjudice de 50 millions 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 considérable selon l'art. 20 ou un préjudice d'au moins 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 tous les services visés à l'art. 2, al. 1 à 3 qui concernent les exigences minimales auxquelles doivent répondre les catégories de sécurité visées à l'art. 17 LSI.

[2] Il tient compte des exigences concernant la sécurité des données sensibles 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 des moyens informatiques suivants doit être contrôlée au moins tous les cinq ans avant leur mise en exploitation, en cas de changements importants durant l'exploitation:

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] Les départements et la Chancellerie fédérale 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 veillent à ce que les responsabilités en matière de sécurité informatique soient définies au niveau opérationnel 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, de la Chancellerie fédérale, des départements et du service spécialisé de la Confédération pour la sécurité de l'information les informations dont ils ont besoin pour assurer la sécurité de l'information.

3 Ils garantissent qu'ils disposent des capacités et compétences personnelles et financières nécessaires pour déceler à temps, procéder à l'analyse technique et à la maîtrise des incidents de sécurité et au traitement des failles de sécurité qui les concernent ou, dans le cadre des conventions visées à l'al. 2, qui concernent leurs bénéficiaires de prestations.

4 Ils procèdent à une surveillance pour s'assurer que l'infrastructure informatique soit utilisée de manière sûre et recherchent régulièrement les menaces et les vulnérabilités. Ils peuvent charger des tiers d'effectuer ces recherches.

5 Le traitements des données personnelles dans le cadre de la surveillance et des recherches visées à l'al. 4 est régie par l'ordonnance du 22 février 2012 sur le traitement des données personnelles liées à l'utilisation de l'infrastructure électronique de la Confédération[12].

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 émet des directives générales et abstraites s'appliquant à tous les services visés à l'art. 2, al. 1 à 3 qui concernent les exigences techniques minimales auxquelles doit satisfaire la vérification, sous l'angle 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[13].

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 garantissent que les collaborateurs faisant l'objet d'un contrôle de sécurité relatif aux personnes visé dans l'ordonnance du … sur les contrôles de sécurité relatifs aux personnes (OCSP)[14] soient sensibilisés chaque année à l'activité sensible déterminante et aux risques qui y sont liés.

2 Les collaborateurs visés à l'al. 1 sont tenus d'annoncer à leur employeur et les circonstances privées professionnelles les empêchant d'accomplir leur activité sensible dans le respect des prescriptions.

12 RS **172.010.442**
13 RS **172.010.59**
14 RS ...

Art. 33 Soupçons 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, les départements transmettent le dossier de l'enquête et les procès-verbaux d'interrogatoire 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 physiques de protection
(art. 22 et 85 LSI)

[1] Après avoir consulté les organes responsables de la sécurité des objets de l'administration fédérale et de l'armée, le service spécialisé de la Confédération pour la sécurité de l'information émet des directives générales et abstraites s'appliquant à tous les services visés à l'art. 2, al. 1 à 3 qui concernent les mesures minimales requises par la 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, et

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

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

[1] Les unités administratives 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] Les locaux et les espaces visés à l'al. 1 ne sont considérés comme des «zones de sécurité» que si l'organe responsable de la sécurité des objets de l'administration fédérale et de l'armée 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 responsables de la sécurité des objets de l'administration fédérale et de l'armée, le service spécialisé de la Confédération pour la sécurité de l'information émet des directives générales et abstraites s'appliquant à tous les services visés à l'art. 2, al. 1 à 3 qui concernent les exigences en matière de sécurité auxquelles doivent répondre les zones de protection et leurs installations.

Section 7 Organisation de sécurité

Art. 36 Responsables de la sécurité de la Chancellerie fédérale et des unités administratives

(art. 7, al. 1, LSI)

1 Le chancelier de la Confédération, les secrétaires généraux et les directeurs des unités de l'administration fédérale centrale et décentralisée sont responsables de la sécurité dans leur domaine de compétence.

2 Ils peuvent déléguer la responsabilité en matière de sécurité 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 la Chancellerie fédérale et des unités administratives 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 importantes qui concernent 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 les mesures de formation et de 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 de l'administration fédérale centrale et décentralisée confient des tâches à leurs préposés à la sécurité de l'information visés à l'art. 37 et veillent à:

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

b. à ce qu'ils ne se voient confier aucune tâche susceptible d'entrer en conflit avec les tâches visées à l'art. 37.

Art. 37 Préposés à la sécurité de l'information des unités administratives

(art. 7, al. 1, LSI)

1 Les unités administratives désignent un ou plusieurs préposés à la sécurité de l'information et leurs suppléants.

2 Les préposés à la sécurité de l'information accomplissent notamment les tâches suivantes:

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

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

c. ils sont le point de contact central des unités administratives pour les questions de sécurité de l'information et conseillent les personnes et les services responsables et les aident à accomplir leurs tâches et devoirs 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 demandent aux responsables de la sécurité de procéder à des mesures de formation et de sensibilisation supplémentaire;

g. ils demandent l'ouverture de la procédure de sécurité relative aux entreprises visée à l'art. 4 de l'ordonnance sur du … sur la procédure de sécurité relative aux entreprises[15];

h. ils coordonnent l'annonce et la maîtrise des incidents de sécurité et le traitement des failles de sécurité dans les unités administratives et auprès des tiers mandatés;

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

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

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

Art. 38 Sécurité de l'information dans les services standard
(art. 7, al. 1, LSI)

1 Le délégué TNI est chargé de garantir la sécurité de l'information dans les services standard visés à l'art. 17, al. 1, let. e, OTNI[16].

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

3 Le préposé à la sécurité de l'information visé à l'al. 2 assume les tâches des services standard visées à l'art. 37, al. 2 et informe l'administration fédérale et l'armée des risques.

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

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

15 RS …
16 RS **172.010.58**

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 des unités administratives;

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

c. ils surveillent le SMSI des unités administratives et collectent les indicateurs nécessaires;

d. ils fixent des objectifs annuels de sécurité pour les unités administratives et vérifient qu'elles les ont atteints;

e. ils veillent au contrôle de la sécurité de l'information en fonction du risque;

f. ils confient des mandats à leurs préposés à la sécurité de l'information visés à l'art. 40 et veillent à:

1. ce qu'ils disposent des compétences et des ressources appropriées,

2. ce qu'ils ne se voient confier aucune tâche susceptible d'entrer en conflit avec les tâches visées à l'art. 40.

3 Ils peuvent assumer les tâches et les compétences que la présente ordonnance attribue aux unités administratives.

4 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 ou de l'unité administrative.

5 Pour autant que les chefs de département n'en décident pas autrement, la sécurité dans le département relève de la responsabilité du secrétaire général qui leur est subordonné.

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 taches 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 et lui demandent de prendre des mesures;

c. ils coordonnent l'annonce et la maîtrise des incidents de sécurité et le traitement des failles de sécurité impliquant plusieurs unités administratives;

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

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

f. ils vérifient périodiquement et en cas de changement ou de départ d'un membre du Conseil fédéral ou du chancelier de la Confédération que les supports d'informations classifiés «secret» soient au complet;

g. ils autorisent l'ouverture de contrôles de sécurité relatifs aux personnes pour les tiers (art. 8, al. 2, let. b, OCSP)[17];

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

Art. 41 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 suivantes pour l'administration fédérale et l'armée:

a. il élabore des stratégies concernant les thèmes dans le domaine de la sécurité;

b. il peut, en cas de projets dans le domaine de la sécurité, demander des informations, prendre position et demander des modifications;

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

d. il prépare des modèles et des aides.

2 Il peut rechercher les menaces techniques et les vulnérabilités dans l'infrastructure informatique de l'administration fédérale et de l'armée ou sur Internet afin d'évaluer et d'améliorer la situation en matière de sécurité de l'information; il peut en charger d'autres services de l'administration fédérale ou de l'armée ou des tiers.

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

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

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

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

c. il peut exécuter les contrôles prévus dans les traités internationaux ou les faire exécuter;

d. il représente la Suisse dans des organismes internationaux;

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

f. il délivre les certificats internationaux de sécurité visés à l'art. 30 OCSP[18].

5 Le service spécialisé de la Confédération pour la sécurité de l'information est rattaché au *[département compétent]*.

17 RS ...
18 RS ...

Section 8 Coûts et évaluation

Art. 42 Coûts

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

2 Les unités administratives garantissent que les coûts sont 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 100 francs pour établir et envoyer les certificats internationaux de sécurité visés à art. 30 OCSP[19] des personnes qui n'accomplissent aucune activité sensible de la Confédération.

Art. 43 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 à la Confédération.

Section 9 Traitement des informations et des données personnelles

Art. 44 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 garantie de 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 les organisations nationales, internationales et étrangères du droit public et privé, dans la mesure où:

a. aucune obligation de maintien du secret légale ou contractuelle n'est violée, et

b. les prescriptions de la législation fédérale en matière de protection des données sont respectées.

3 Pour autant que cela soit nécessaire pour maîtriser un incident de sécurité ou traiter une faille de sécurité, elles peuvent également traiter et échanger des données sensibles relatives à l'identité et aux actes des personnes ayant participé à l'incident ou qui sont concernées par l'incident ou qui pourraient y avoir participé ou être concernées.

19 RS **126.xxx**

Art. 45 Application SMSI

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

[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. 4, al. 3.

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

Art. 46 Services électroniques de formulaire

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

a. gérer les voyages visés à l'art. 41, al. 4, let. e;

b. établir et envoyer les certificats internationaux de sécurité visés à l'art. 30 OCSP[20];

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

[2] Les données personnelles figurant dans l'annexe 2 peuvent être traitées à l'aide des services de formulaires 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 les 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 formulaires visés à l'al. 3, elles peuvent traiter les données personnelles, y compris les données sensibles, visées à l'art. 44, al. 3, qui sont nécessaires à la maîtrise des incidents de sécurité et au traitement des failles de sécurité.

[5] Les données visées à l'al. 4 doivent être effacées du service de formulaire immédiatement après l'envoi de l'annonce. Elles peuvent provisoirement être enregistrées avant l'envoi durant 24 heures au plus.

Section 10 Dispositions finales

Art. 47 Abrogation et modification d'autres actes

[1] Sont abrogées:

a. l'ordonnance du 27 mai 2020 sur les cyberrisques[21];

20 RS **128.xxx**
21 [RO **2020** 2107, **2020** 5871, **2021** 132]

b. l'ordonnance du 4 juillet 2007 concernant la protection des informations[22].

2 La modification d'autres actes est réglée dans l'annexe 3.

Art. 48 Dispositions transitoires

1 Les directives en matière de sécurité informatique émises par le Centre national pour la cybersécurité et les exceptions qu'il a autorisées avant l'entrée en vigueur de la présente ordonnance conservent leur validité durant six 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 prend les décisions concernant les changements des consignes et des exceptions autorisées.

3 Les directives en matière de sécurité informatique 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 cinq ans au plus après l'entrée en vigueur de la présente ordonnance.

4 Les unités administratives et la Chancellerie fédérale mettent en place leur SMSI au plus tard trois ans après l'entrée en vigueur de la présente ordonnance.

5 L'accréditation de sécurité visée à l'art. 23 n'est pas effectuée pour les moyens informatiques qui:

a. sont en service avant l'entrée en vigueur de la présente ordonnance;

b. sont en développement au moment de l'entrée en vigueur de la présente ordonnance, dans la mesure où elle entraînerait une charge de travail disproportionnée.

Art. 49 Entrée en vigueur

La présente ordonnance entre en vigueur le … 2023.

… Au nom du Conseil fédéral suisse:

Le président de la Confédération, …
Le chancelier de la Confédération, Walter Thurnherr

22 [RO **2007** 3401, **2010** 3207, **2013** 1341, **2014** 3543, **2016** 1785, **2017** 7391, **2020** 6011]

Annexe 1
(art. 2, al. 2 et 3)

Unités de l'administration fédérale décentralisée auxquelles s'applique l'ordonnance sur la sécurité de l'information ou certaines de ses parties

1. Unités administratives qui ont accès aux moyens informatiques des fournisseurs internes de prestations informatiques visés à l'art. 9 OTNI[23] relevant des catégories de sécurité «protection élevée» ou «protection très élevée» visées à l'art. 28 (cf. art. 2, al. 2, let. a):

a. …

b. …

c. …

2. Unités administratives qui utilisent les moyens informatiques relevant des catégories de sécurité «protection élevée» ou «protection très élevée» visées à l'art. 28 (cf. art. 2, al. 2, let. b)

a. …

b. …

c. …

3. Unités administratives qui ne sont pas concernées par les let. a et b, mais qui traitent des informations classifiées de la Confédération (cf. art. 2, al. 2, let. c):

a. …

b. …

c. …

4. Autres unités administratives (cf. art. 2, al. 3):

a. …

b. …

c. …

23 RS **172.010.58**

Annexe 2
(art. 46, al. 2)

Traitement des données dans les services de formulaire visés à l'art. 46

Les données personnelles suivantes peuvent être traitées dans les services de formulaire visés à l'art. 46:

1. Service de formulaire visé à l'art. 46, al. 1, let. a, OSI
   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. Nationalité/s*
      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 coordonnés 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 munies d'un astérisque (*) sont communiquées à l'autorité de sécurité étrangère.

2. Service de formulaire visé à l'art. 46, al. 1, let. b, OSI

   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 nom de la personne de référence au sein de l'organisation ou de l'armée
      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 autres coordonnées, en particulier électroniques, de la personne de référence
      5. Motif de l'établissement du certificat

3. Service de formulaire visé à l'art. 46, al. 1, let. c, OSI

   a. Données relatives à l'entreprise:
      1. Nom complet*
      2. Forme juridique*
      3. Numéro d'identification des entreprises
      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, numéros de téléphone et autres coordonnées, en particulier électroniques, de la personne de référence

b. Données concernant le certificat de sécurité:
   1. Date d'établissement et durée de validité*
   2. Champ d'application et charges*
   3. Catégorie de classification ou de sécurité la plus élevée autorisée*

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

4. Service de formulaire visé à l'art. 46, al. 3 à 5, OSI

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 3
(art. 47, al. 2)

Modification d'autres actes

Les actes mentionnés ci-après sont modifiés comme suit:

1. Ordonnance du 25 novembre 2020 sur la coordination de la transformation numérique et la gouvernance de l'informatique dans l'administration fédérale[24]

Art. 2, al. 2, phrase introductive

2 Peuvent, sous réserve d'autres dispositions d'organisation contenues dans le droit fédéral, se soumettre par un accord avec le secteur Transformation numérique et gouvernance de l'informatique de la Chancellerie fédérale (secteur TNI de la ChF) à la présente ordonnance, à l'ordonnance du […] sur la sécurité de l'information[25] et à l'ordonnance GEVER du 3 avril 2019[26], y compris aux directives fondées sur celles-ci:

2. Ordonnance du 7 mars 2003 sur l'organisation du Département fédéral de la défense, de la protection de la population et des sports[27]

Art. 3, al. 2

2 Il édicte des prescriptions en vue de garantir l'équipement de l'armée.

Art. 6, let. b

Abrogée

3. Ordonnance du 24 juin 2009 concernant les relations militaires internationales[28]

Art. 4, let. c

Les services suivants peuvent établir formellement des relations militaires internationales dans leur domaine d'activités sans autorisation du Protocole militaire:

c. le service spécialisé de la Confédération pour la sécurité de l'information;

24 RS **172.010.58**
25 RS …
26 RS **172.010.441**
27 RS **172.214.1**
28 RS **510.215**

Art. 5, al. 1

[1] La remise d'informations classifiées à des personnes ou à des organes étrangers et l'accès à des informations militaires classifiées, à du matériel classifié ou à des installations militaires en Suisse par des personnes étrangères sont soumis aux dispositions régissant la protection de l'information, notamment:

a. le traité international applicable dans le cas concret visé à l'art. 87 de la loi du 20 décembre 2020 sur la sécurité de l'information[29];

b. l'ordonnance du … sur les contrôles de sécurité relatif aux personnes[30];

c. l'ordonnance du … sur la sécurité de l'information[31];

d. l'ordonnance du … sur la procédure de sécurité relative aux entreprises[32].

29 RS **128**
30 RS **...**
31 RS **...**
32 RS **...**