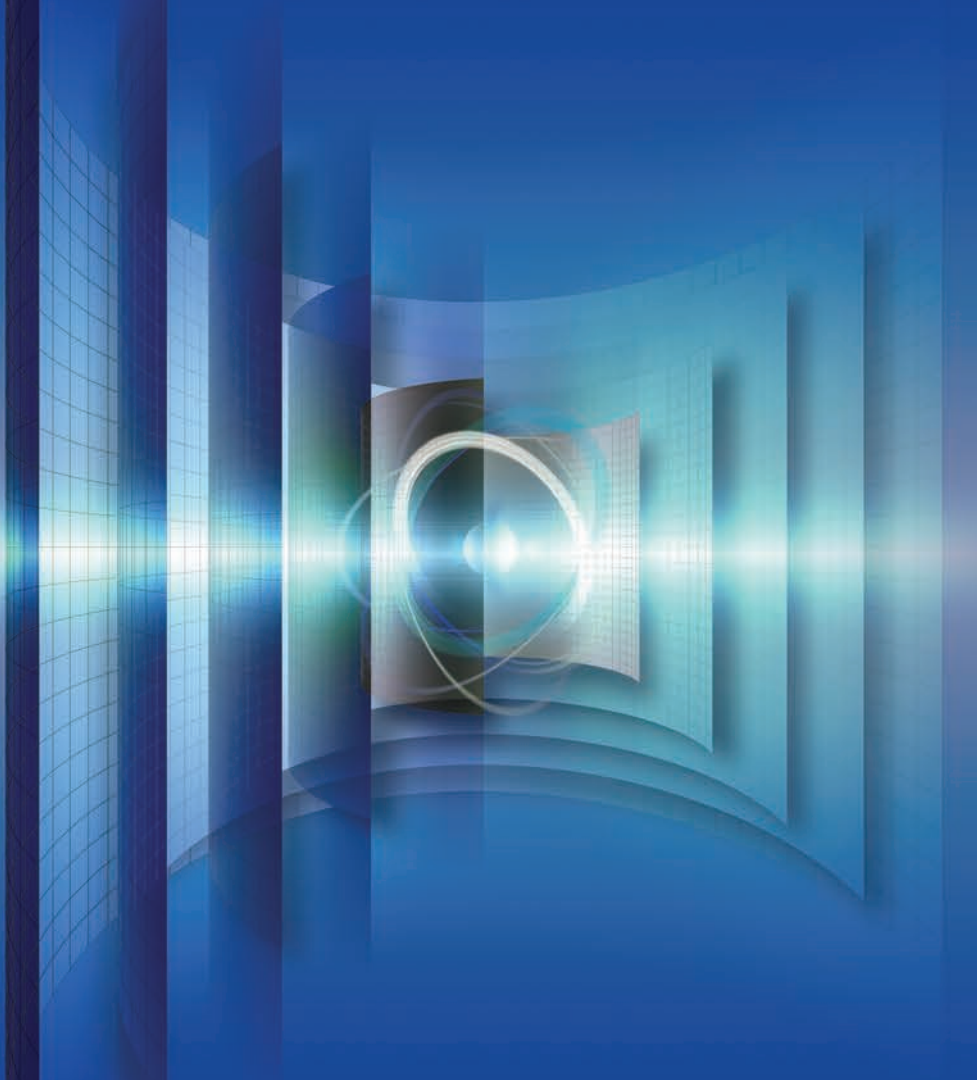
Collection Sécurité nucléaire de l'AIEA – n° 23-G

Guide d'application

Sécurité de l'information nucléaire



IAEA
Agence internationale de l'énergie atomique

LA COLLECTION SÉCURITÉ NUCLÉAIRE DE L'AIEA

Les publications de la **collection Sécurité nucléaire de l'AIEA** traitent des mesures à prendre en matière de prévention, de détection et d'intervention contre le vol, le sabotage et la cession illégale de matières nucléaires et de sources radioactives et des installations connexes, l'accès non autorisé à ces matières, sources et installations et les autres actes malveillants dont elles peuvent faire l'objet. Ces publications sont conformes aux instruments internationaux relatifs à la sécurité nucléaire, notamment à la Convention sur la protection physique des matières nucléaires telle qu'amendée, au Code de conduite sur la sûreté et la sécurité des sources radioactives, aux résolutions 1373 et 1540 du Conseil de sécurité des Nations Unies et à la Convention internationale pour la répression des actes de terrorisme nucléaire, et elles les complètent.

CATÉGORIES DANS LA COLLECTION SÉCURITÉ NUCLÉAIRE DE L'AIEA

Les publications de la collection Sécurité nucléaire de l'AIEA se répartissent entre les catégories suivantes :

- Les **Fondements de la sécurité nucléaire**, qui énoncent les objectifs, les concepts et les principes de la sécurité nucléaire et servent de base pour l'élaboration de recommandions en matière de sécurité.
- Les **Recommandations**, qui présentent les pratiques exemplaires que les États Membres devraient adopter pour la mise en œuvre des Fondements de la sécurité nucléaire.
- Les **Guides d'application**, qui complètent les Recommandations dans certains grands domaines et proposent des mesures pour en assurer la mise en œuvre.
- Les **Orientations techniques**, comprenant les **Manuels de référence**, qui présentent des mesures détaillées et/ou donnent des conseils pour la mise en œuvre des Guides d'application dans des domaines ou des activités spécifiques, les **Guides de formation**, qui présentent les programmes et/ou les manuels des cours de formation de l'AIEA dans le domaine de la sécurité nucléaire, et les **Guides des services**, qui donnent des indications concernant la conduite et la portée des missions consultatives de l'AIEA sur la sécurité nucléaire.

RÉDACTION ET EXAMEN

Des experts internationaux aident le Secrétariat de l'AIEA à élaborer ces publications. Pour l'élaboration des Fondements de la sécurité nucléaire, des Recommandations et des Guides d'application, l'AIEA organise des réunions techniques à participation non limitée afin que les États Membres intéressés et les organisations internationales compétentes puissent examiner comme il se doit les projets de texte. En outre, pour faire en sorte que ces projets soient examinés de façon approfondie et largement acceptés au niveau international, le Secrétariat les soumet aux États Membres, qui disposent de 120 jours pour les examiner officiellement, ce qui leur donne la possibilité d'exprimer pleinement leurs vues avant que le texte soit publié.

Les publications de la catégorie Orientations techniques sont élaborées en consultation étroite avec des experts internationaux. Il n'est pas nécessaire d'organiser des réunions techniques, mais on peut le faire lorsque cela est jugé nécessaire pour recueillir un large éventail de points de vue.

Le processus d'élaboration et d'examen des publications de la collection Sécurité nucléaire de l'AIEA tient compte des considérations de confidentialité et du fait que la sécurité nucléaire est indissociable des problèmes généraux et spécifiques concernant la sécurité nationale. La prise en compte, dans le contenu technique des publications, des normes de sûreté et des activités de garanties de l'AIEA se rapportant à la sécurité constitue une préoccupation sous-jacente.

SÉCURITÉ DE L'INFORMATION NUCLÉAIRE

Les États ci-après sont Membres de l'Agence internationale de l'énergie atomique :

AFGHANISTAN
AFRIQUE DU SUD
ALBANIE
ALGÉRIE
ALLEMAGNE
ANGOLA
ANTIGUA-ET-BARBUDA
ARABIE SAOUDITE
ARGENTINE
ARMÉNIE
AUSTRALIE
AUTRICHE
AZERBAÏDJAN
BAHAMAS
BAHREÏN
BANGLADESH
BARBADE
BÉLARUS
BELGIQUE
BELIZE
BÉNIN
BOLIVIE, ÉTAT PLURINATIONAL DE
BOSNIE-HERZÉGOVINE
BOTSWANA
BRÉSIL
BRUNÉI DARUSSALAM
BULGARIE
BURKINA FASO
BURUNDI
CAMBODGE
CAMEROUN
CANADA
CHILI
CHINE
CHYPRE
COLOMBIE
CONGO
CORÉE, RÉPUBLIQUE DE
COSTA RICA
CÔTE D'IVOIRE
CROATIE
CUBA
DANEMARK
DJIBOUTI
DOMINIQUE
ÉGYPTE
EL SALVADOR
ÉMIRATS ARABES UNIS
ÉQUATEUR
ÉRYTHRÉE
ESPAGNE
ESTONIE
ÉTATS-UNIS D'AMÉRIQUE
ÉTHIOPIE
FÉDÉRATION DE RUSSIE
FIDJI
FINLANDE
FRANCE
GABON
GÉORGIE
GHANA
GRÈCE
GUATEMALA
GUYANA
HAÏTI
HONDURAS
HONGRIE
ÎLES MARSHALL
INDE
INDONÉSIE
IRAN, RÉP. ISLAMIQUE D'
IRAQ
IRLANDE
ISLANDE
ISRAËL
ITALIE
JAMAÏQUE
JAPON
JORDANIE
KAZAKHSTAN
KENYA
KIRGHIZISTAN
KOWEÏT
LESOTHO
LETTONIE
L'EX-RÉPUBLIQUE YOUGOSLAVE DE MACÉDOINE
LIBAN
LIBÉRIA
LIBYE
LIECHTENSTEIN
LITUANIE
LUXEMBOURG
MADAGASCAR
MALAISIE
MALAWI
MALI
MALTE
MAROC
MAURICE
MAURITANIE
MEXIQUE
MONACO
MONGOLIE
MONTÉNÉGRO
MOZAMBIQUE
MYANMAR
NAMIBIE
NÉPAL
NICARAGUA
NIGER
NIGERIA
NORVÈGE
NOUVELLE-ZÉLANDE
OMAN
OUGANDA
OUZBÉKISTAN
PAKISTAN
PALAOS
PANAMA
PAPOUASIE-NOUVELLE-GUINÉE
PARAGUAY
PAYS-BAS
PÉROU
PHILIPPINES
POLOGNE
PORTUGAL
QATAR
RÉPUBLIQUE ARABE SYRIENNE
RÉPUBLIQUE CENTRAFRICAINE
RÉPUBLIQUE DE MOLDOVA
RÉPUBLIQUE DÉMOCRATIQUE DU CONGO
RÉPUBLIQUE DÉMOCRATIQUE POPULAIRE LAO
RÉPUBLIQUE DOMINICAINE
RÉPUBLIQUE TCHÈQUE
RÉPUBLIQUE-UNIE DE TANZANIE
ROUMANIE
ROYAUME-UNI DE GRANDE-BRETAGNE ET D'IRLANDE DU NORD
RWANDA
SAINT-MARIN
SAINT-SIÈGE
SÉNÉGAL
SERBIE
SEYCHELLES
SIERRA LEONE
SINGAPOUR
SLOVAQUIE
SLOVÉNIE
SOUDAN
SRI LANKA
SUÈDE
SUISSE
SWAZILAND
TADJIKISTAN
TCHAD
THAÏLANDE
TOGO
TRINITÉ-ET-TOBAGO
TUNISIE
TURKMÉNISTAN
TURQUIE
UKRAINE
URUGUAY
VANUATU
VENEZUELA, RÉP. BOLIVARIENNE DU
VIET NAM
YÉMEN
ZAMBIE
ZIMBABWE

Le Statut de l'Agence a été approuvé le 23 octobre 1956 par la Conférence sur le Statut de l'AIEA, tenue au Siège de l'Organisation des Nations Unies, à New York ; il est entré en vigueur le 29 juillet 1957. L'Agence a son Siège à Vienne. Son principal objectif est « de hâter et d'accroître la contribution de l'énergie atomique à la paix, la santé et la prospérité dans le monde entier ».

COLLECTION
SÉCURITÉ NUCLÉAIRE DE L'AIEA nº 23-G

SÉCURITÉ DE L'INFORMATION NUCLÉAIRE

GUIDE D'APPLICATION

AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE
VIENNE, 2017

NOTE CONCERNANT LE DROIT D'AUTEUR

Unité de la promotion et de la vente, Section d'édition
Agence internationale de l'énergie atomique
Centre international de Vienne
BP 100
1400 Vienne, Autriche
télécopie : +43 1 2600 29302
téléphone : +43 1 2600 22417
courriel : sales.publications@iaea.org
http://www.iaea.org/books

Imprimé par l'AIEA en Autriche
Juillet 2017
STI/PUB/1677

SÉCURITÉ DE L'INFORMATION NUCLÉAIRE

AIEA, VIENNE, 2017
STI/PUB/1677
ISBN 978–92–0–204317–6
ISSN 2520–6931

AVANT-PROPOS

de Yukiya Amano
Directeur général

Aux termes de son statut, le principal objectif de l'AIEA est « de hâter et d'accroître la contribution de l'énergie atomique à la paix, la santé et la prospérité dans le monde entier ». Notre travail consiste à la fois à prévenir la dissémination des armes nucléaires et à faire en sorte que les techniques nucléaires soient accessibles à des fins pacifiques dans des domaines comme la santé ou l'agriculture. Il est essentiel que toutes les matières nucléaires et les autres matières radioactives, ainsi que les installations dans lesquelles elles sont conservées, soient gérées de manière sûre et convenablement protégées contre les actes criminels et les autres actes délibérés non autorisés.

La sécurité nucléaire est de la responsabilité de chaque État, mais la coopération internationale est indispensable pour aider les pays à établir et à maintenir des régimes de sécurité nucléaire efficaces. Le rôle central que joue l'AIEA pour faciliter cette coopération et aider les États est bien connu. Ce rôle s'explique par le nombre élevé d'États Membres de l'Agence, par son mandat, par sa compétence unique et par sa longue expérience en matière d'assistance technique et d'orientations pratiques spécialisées destinées aux États.

En 2006, l'AIEA a créé la collection Sécurité nucléaire afin d'aider les États à établir des régimes de sécurité nucléaire nationaux efficaces. Les publications qu'elle a fait paraître dans ce cadre complètent les instruments juridiques internationaux sur la sécurité nucléaire, comme la Convention sur la protection physique des matières nucléaires et son amendement, la Convention internationale pour la répression des actes de terrorisme nucléaire, les résolutions 1373 et 1540 du Conseil de sécurité de l'ONU et le Code de conduite sur la sûreté et la sécurité des sources radioactives.

Des experts des États Membres de l'AIEA participent activement à l'élaboration des orientations afin que celles-ci reflètent un consensus sur les bonnes pratiques à appliquer en matière de sécurité nucléaire. Le Comité des orientations sur la sécurité nucléaire, créé par l'AIEA en mars 2012 et constitué de représentants des États Membres, examine et approuve les projets de publications de la collection Sécurité nucléaire au fur et à mesure de leur élaboration.

L'AIEA continuera d'œuvrer avec ses États Membres pour que les bienfaits des techniques nucléaires pacifiques contribuent à améliorer la santé, le bien-être et la prospérité des peuples du monde entier.

NOTE DE L'ÉDITEUR

Les États ne sont pas tenus d'appliquer les orientations publiées dans la collection Sécurité nucléaire de l'AIEA, mais elles peuvent les aider à s'acquitter de leurs obligations en vertu d'instruments juridiques internationaux et assumer leurs responsabilités en matière de sécurité nucléaire au sein de l'État. Les orientations énoncées au conditionnel ont pour but de présenter des bonnes pratiques internationales et de manifester un consensus international selon lequel il est nécessaire pour les États de prendre les mesures recommandées ou des mesures équivalentes.

Les termes relatifs à la sécurité ont le sens donné dans la publication où ils figurent, ou dans les orientations de niveau supérieur que la publication soutient. Autrement, les termes ont le sens qui leur est communément donné.

Un appendice est réputé faire partie intégrante de la publication. Les informations données dans un appendice ont le même statut que le corps du texte. Les annexes ont pour objet de donner des exemples concrets ou des précisions ou explications. Elles ne sont pas considérées comme faisant partie intégrante du texte principal.

Bien que l'exactitude des informations contenues dans la présente publication ait fait l'objet d'un soin particulier, ni l'AIEA ni ses États Membres n'assument une quelconque responsabilité pour les conséquences éventuelles de leur utilisation.

L'emploi d'appellations particulières pour désigner des pays ou des territoires n'implique de la part de l'éditeur, l'AIEA, aucune prise de position quant au statut juridique de ces pays ou territoires, ou de leurs autorités et institutions, ni quant au tracé de leurs frontières.

La mention de noms de sociétés ou de produits particuliers (qu'ils soient ou non signalés comme marques déposées) n'implique aucune intention d'empiéter sur des droits de propriété et ne doit pas être considérée non plus comme valant approbation ou recommandation de la part de l'AIEA.

TABLE DES MATIÈRES

1. INTRODUCTION

GÉNÉRALITÉS

1.1. L'objectif général d'un régime national de sécurité nucléaire est de protéger les personnes, les biens, la société et l'environnement contre les conséquences néfastes d'un événement de sécurité nucléaire [1]. L'accès à des informations sensibles peut être utile aux groupes ou aux individus qui souhaitent préparer ou commettre un acte malveillant mettant en jeu des matières nucléaires, d'autres matières radioactives ou les installations associées. Ces informations devraient donc être recensées, classées et protégées par des mesures appropriées. Une information sensible, quelle que soit sa forme, logiciel inclus, est une information dont la divulgation, la modification, la transformation, la destruction ou le refus d'utilisation non autorisés pourraient compromettre la sécurité nucléaire.

1.2. La confidentialité est la propriété selon laquelle une information n'est pas rendue accessible ou divulguée à des personnes, entités ou processus non autorisés. La sécurité de l'information ne se limite pas à la confidentialité de l'information, mais comprend également l'exactitude et l'exhaustivité de l'information (son intégrité), ainsi que son accessibilité ou la possibilité de l'utiliser à la demande (sa disponibilité).

1.3. Assurer la sécurité des informations sensibles est une condition transversale préalable à la sécurité nucléaire et les dispositifs et les mesures permettant d'atteindre une sécurité de l'information efficace sont des éléments essentiels d'un régime national de sécurité nucléaire.

1.4. Dans les Fondements de la sécurité nucléaire [1] et les trois Recommandations de sécurité nucléaire publiées [2 à 4], l'importance de la protection des informations sensibles est prise en compte. Le présent guide d'application complète les notions générales exposées dans ces publications afin d'expliquer plus en détail ce qu'il convient de faire.

OBJET

1.5. La présente publication donne des conseils sur l'application du principe de confidentialité et sur la question plus large de la sécurité de l'information. Concernant l'instauration et la gestion d'un régime de sécurité de l'information pour divers types d'informations, tant sous forme d'orientations de haut niveau

que de normes détaillées, de nombreuses orientations nationales et internationales existent déjà. L'objet de la présente publication n'est donc pas de s'y substituer. Il est au contraire d'aider les États à faire le lien entre les normes nationales et sectorielles en vigueur concernant la sécurité de l'information en général, les considérations et les concepts particuliers qui s'appliquent à la sécurité nucléaire et les dispositions et conditions spécifiques aux matières nucléaires et aux autres matières radioactives.

1.6. L'objet de la présente publication est de donner des orientations concernant :

a) l'instauration d'un cadre efficace pour garantir la confidentialité, l'intégrité et la disponibilité des informations sensibles (section 3), notamment la législation et la réglementation nécessaires ;
a) le choix des informations qui peuvent être considérées comme sensibles (section 4) ;
a) les considérations relatives à la mise en commun et à la divulgation des informations sensibles (section 5) ;
b) les principes directeurs et les méthodes permettant de garantir la confidentialité, l'intégrité et la disponibilité des informations (section 6).

CONTENU

1.7. La présente publication porte sur la sécurité des informations sensibles qui concernent les usages civils des matières nucléaires et des autres matières radioactives, ainsi que les installations et activités associées. Elle traite essentiellement des informations sensibles relatives aux matières et aux installations soumises à un contrôle réglementaire.

1.8. S'agissant des matières nucléaires et des autres matières radioactives non soumises à un contrôle réglementaire, la sécurité nucléaire peut également s'appliquer à des informations sensibles qui doivent être protégées. En pareil cas, il conviendrait de suivre les orientations générales présentées ici dans la mesure où elles seront pertinentes.

1.9. La présente publication s'adresse à toutes les personnes qui sont responsables de la sécurité d'informations sensibles et notamment :

a) les autorités compétentes, y compris les organismes de réglementation ;

b) le personnel d'encadrement des installations, des sociétés et des organisations qui jouent un rôle dans l'utilisation, l'entreposage ou le transport de matières nucléaires ou d'autres matières radioactives ;
c) les exploitants d'installations et leur personnel, en particulier le personnel de sécurité ;
d) les entreprises et les autres personnes qui travaillent pour les autorités, les organisations ou les exploitants d'installations ;
e) toutes les autres entités qui ont légitimement accès à des informations sensibles.

STRUCTURE

1.10. À la suite de l'introduction, la section 2 présente plusieurs termes et concepts essentiels qui seront utilisés dans toute la publication. La section 3 décrit les éléments nécessaires à l'instauration d'un cadre national relatif à la sécurité des informations sensibles et les sections 4 à 6 examinent ces éléments à tour de rôle. La section 4 présente les points à prendre en considération pour déterminer quelles sont les informations qui sont sensibles et doivent donc être protégées. La section 5 expose les facteurs en prendre en compte concernant la mise en commun et la divulgation d'informations sensibles. La section 6 décrit plus en détail les mesures qui doivent être prises au niveau des installations pour protéger les informations sensibles. L'annexe I donne un exemple de système de classification et l'annexe II présente un exemple de catégorisation relative à la sécurité pour les informations ayant trait à la sécurité nucléaire. Enfin, l'annexe III propose un cadre et un contenu pour un programme de formation et de sensibilisation.

2. CONCEPTS ET CONTEXTE

2.1. La présente section clarifie le sens de certains termes importants qui sont employés dans le texte. Elle applique également les concepts essentiels de la sécurité de l'information au contexte de la sécurité nucléaire. Les définitions d'un plus grand nombre de termes utiles figurent dans le glossaire qui se trouve à la fin de la présente publication.

INFORMATIONS

2.2. Les informations sont de la connaissance, quelle que soit la forme sous laquelle elles existent ou sont exprimées. Elles comprennent les idées, les concepts, les événements, les processus, les pensées, les faits et les schémas. Une information peut être enregistrée sur des supports tels que papier, pellicule et supports magnétiques ou optiques ou être conservée dans un appareil électronique. Elle peut être représentée et communiquée par presque n'importe quel moyen. Dans le domaine nucléaire, il existe une grande quantité d'informations présentées sous de multiples formes. Les actifs informationnels sont les appareils ou les éléments (supports inclus) qui sont utilisés pour stocker, traiter, contrôler ou transmettre des informations.

2.3. Pour des besoins d'exploitation et de sécurité, les informations peuvent être regroupées en objets informationnels. Ces derniers peuvent se définir comme les éléments d'information qui ont de la valeur pour une organisation. Un objet informationnel comprend généralement un ensemble de données, d'informations ou de connaissances ayant en commun une utilisation, un objet, un risque associé ou une forme de stockage ou de transmission.

2.4. Il importe de comprendre que les informations liées à la sécurité nucléaire peuvent avoir une valeur (de natures et d'importances éventuellement diverses) pour tout ou partie des acteurs suivants :

a) l'État ;
b) les autorités compétentes ;
c) les exploitants d'installations (y compris les tiers, par exemple les vendeurs) ;
d) un adversaire potentiel (individu ou entité organisée) ;
e) les médias ;
f) le public.

RECENSEMENT ET PROTECTION DES INFORMATIONS SENSIBLES

2.5. Une information sensible est une information dont la divulgation (ou la modification, la transformation, la destruction ou le refus d'utilisation) non autorisée pourrait compromettre la sécurité nucléaire ou faciliter la commission d'un acte malveillant contre une installation, une organisation ou un transport nucléaires. Une telle information peut par exemple concerner les mesures de sécurité nucléaire au niveau d'une installation, les structures, systèmes

et composants d'une installation, l'emplacement et le transport de matières nucléaires ou d'autres matières radioactives ou le personnel d'une organisation.

2.6. Le recensement des informations qui répondent à cette définition fait partie des étapes indispensables à accomplir pour pouvoir établir un programme de sécurité de l'information afin d'assurer la confidentialité des informations. La section 4 contient des orientations plus détaillées et plus complètes sur cette question et l'annexe II présente des exemples à titre d'illustration.

2.7. La protection des informations sensibles est une nécessité. En effet, la possibilité d'accéder facilement à des informations insuffisamment protégées peut aider des adversaires à préparer ou à commettre un acte malveillant sans qu'ils déploient beaucoup d'efforts ou ne prennent trop de risques. Si, par exemple, des adversaires projetant d'attaquer une installation se procuraient le plan de protection physique de l'installation en question, ils sauraient d'emblée quels obstacles ils auraient à franchir et connaîtraient le nombre et l'armement des agents de sécurité, l'effectif de la force d'intervention et le temps approximativement nécessaire à cette dernière pour arriver sur le site. Ils connaîtraient également l'emplacement des cibles importantes au sein d'une installation, ainsi que les mesures qui les protègent. De même, si un adversaire qui souhaite voler des matières nucléaires durant un transport parvenait à trouver un dispositif donnant accès à des informations détaillées sur le transport prévu – du fait que ce dispositif n'aurait pas été suffisamment protégé –, il pourrait préparer une attaque plus efficacement. Le fait que des adversaires possèdent de telles informations ou de tels actifs informationnels augmente donc leurs chances de réussite.

2.8. L'accès aux informations et aux objets informationnels sensibles devrait se limiter à ce qui est nécessaire à la conduite des activités d'une organisation. Par conséquent, ces éléments ne devraient être communiqués qu'aux seules personnes dûment autorisées et seulement lorsqu'elles ont besoin d'y avoir accès. Les règles du « besoin d'en connaître » et du « besoin de détenir » sont fondamentales pour la sécurité des informations sensibles. Elles devraient éclairer la gestion et le contrôle des droits d'accès aux informations. Ces droits devraient être réexaminés à intervalles réguliers et lorsque cela est prescrit.

2.9. Le respect de la confidentialité dépend de l'application de mesures de sécurité aux informations considérées comme sensibles et aux ressources d'informations considérées comme sensibles (appareils ou éléments, supports inclus, qui servent à traiter, exploiter, stocker ou transmettre des informations sensibles) afin qu'ils ne tombent pas entre les mains de personnes ou

d'organisation non autorisées, qu'elles soient externes ou internes. On trouvera des orientations sur les mesures contre les menaces internes dans la publication intitulée *Mesures de prévention et de protection contre les menaces internes* [5]. Les mesures de sécurité devraient être définies à partir d'une analyse des risques, qui devrait être actualisée grâce à des examens périodiques.

SÉCURITÉ DE L'INFORMATION

2.10. Dans la présente publication, la sécurité de l'information désigne le régime, le programme ou l'ensemble de règles mis en place pour assurer la confidentialité, l'intégrité et la disponibilité de l'information sous toutes ses formes. Elle comprend au minimum :

a) la sécurité des informations présentées sous forme physique (papier et supports électroniques, par exemple) ;
b) la sécurité des systèmes informatiques, parfois appelée sécurité informatique ou cybersécurité (on trouvera des orientations complémentaires dans la publication de l'AIEA intitulée *La sécurité informatique dans les installations nucléaires* [6]) ;
c) la sécurité des actifs informationnels (comme le matériel de stockage et de traitement des informations, les systèmes de communication, et les réseaux) ;
d) la sécurité des informations relatives au personnel des installations et à d'autres personnes (par exemple les entreprises ou les vendeurs) qui pourraient compromettre la sécurité de ce qui précède ;
e) la sécurité des informations immatérielles (comme les connaissances).

2.11. La confidentialité est souvent mise en avant, mais les organisations devraient faire en sorte que leur programme de sécurité de l'information porte sur les trois aspects. La perte d'intégrité ou de disponibilité peut avoir une incidence néfaste sur la sécurité nucléaire au même titre que la perte de confidentialité. Tel est par exemple le cas si des utilisateurs autorisés n'ont pas accès aux informations nécessaires à l'exercice de leur fonction en temps opportun (perte de disponibilité) ou si ces informations ont été transformées au point d'induire ces utilisateurs en erreur (perte d'intégrité).

2.12. La sécurité de l'information devrait être envisagée et assurée dans le cadre du régime général de sécurité. Elle est intimement liée à d'autres domaines de la sécurité comme la protection physique et les habilitations de sécurité. Des mesures de protection physique peuvent par exemple servir à protéger des

informations sensibles et des ressources d'informations sensibles, tandis que des mesures de confidentialité rendent les attaques contre les systèmes de protection physique plus difficiles ou leur issue plus incertaine pour des adversaires. Des carences dans l'un quelconque des domaines de la sécurité peuvent avoir des répercussions sur la sécurité des autres domaines. Il est donc indispensable d'adopter une approche globale en examinant simultanément l'ensemble des domaines.

2.13. En matière de sécurité de l'information, il convient également de tenir compte de l'équilibre nécessaire entre la sécurité et d'autres objectifs, notamment la sûreté, l'ouverture, la transparence et les aspects opérationnels. On trouvera des orientations sur la sûreté dans la collection Normes de sûreté de l'AIEA.

3. CADRE DE PROTECTION DES INFORMATIONS SENSIBLES

3.1. Il n'est pas efficace de protéger les informations sensibles de manière fragmentaire, installation par installation. Un cadre national efficace est nécessaire pour que des mesures de sécurité complètes s'appliquent dans tous les sites, installations et organisations (gouvernementales et non gouvernementales) qui exploitent des informations sensibles. L'État devrait construire ce cadre national, ce qui nécessitera d'établir :

a) la responsabilité de l'État ;
b) un cadre législatif et réglementaire ;
c) des orientations nationales ;
d) des politiques de sécurité ;
e) des systèmes de classification.

Les politiques mises en œuvre au sein de chaque organisation font également partie du cadre global.

RESPONSABILITÉS

3.2. L'existence et le fonctionnement efficace d'un régime national complet de sécurité incombent au gouvernement de l'État concerné. Le fait de garantir la

sécurité des informations sensibles fait partie intégrante du régime de sécurité nucléaire que l'État devrait faire appliquer.

3.3. Les États disposent généralement d'organismes ou d'organes qui sont responsables de la sécurité nationale globale et qui seront appelés autorités nationales de sécurité dans la suite de la présente publication. Ces autorités ont habituellement pour tâche de définir la politique nationale fondamentale sur tous les aspects de la sécurité. Les politiques et les consignes de sécurité qu'elles établissent ont souvent un caractère général et n'ont pas été conçues spécifiquement pour la sécurité nucléaire. Toutefois, dans de nombreux États, les autorités nationales de sécurité disposent de politiques et d'orientations relatives à la protection des informations sensibles, par exemple dans l'administration ou dans l'armée.

3.4. Les autorités compétentes devraient élaborer et publier une politique et des prescriptions spécifiques pour la sécurité des informations sensibles dans les installations et pour les activités associées à des matières nucléaires ou à d'autres matières radioactives. Cette politique et ces prescriptions s'appuient généralement sur la politique et les prescriptions de sécurité nationale établies par les autorités nationales de sécurité et sont conformes à cette politique et à ces règles, mais tiennent compte de la nature particulière des activités qui mettent en jeu de telles matières. Les autorités compétentes devraient également maintenir des liens étroits avec les autorités nationales de sécurité afin de mettre en œuvre une évaluation nationale de la menace ou de définir la menace de référence (pour de plus amples informations, consulter la publication intitulée Élaboration, utilisation et actualisation de la menace de référence [7]).

3.5. Chaque organisation devrait établir sa politique, ses plans et ses procédures internes pour garantir la confidentialité, l'intégrité et la disponibilité de toutes les informations sensibles relatives à la sécurité nucléaire qu'elle détient ou exploite et pour protéger les ressources d'informations sensibles qui y sont associées, conformément à la politique de sécurité nationale et aux lois et prescriptions applicables. Tous les salariés devraient être pleinement conscients de l'importance de la sécurité de l'information et suivre les règles et les procédures adoptées par leur employeur dans ce domaine.

CADRE LÉGISLATIF ET RÉGLEMENTAIRE DE PROTECTION DES INFORMATIONS SENSIBLES

3.6. Les prescriptions visant à maintenir la sécurité nucléaire à l'intérieur des frontières d'un État devraient s'appliquer à tous les ministères, directions, organes et autres organisations qui s'occupent de sujets dont l'État considère qu'ils sont utiles pour la sécurité nucléaire nationale. L'État peut imposer ces prescriptions par des lois, des règlements ou d'autres prescriptions juridiquement contraignantes et ces prescriptions devraient notamment porter sur la sécurité de l'information. Une loi en vigueur devrait aussi déterminer les sanctions ou les peines encourues par une personne ou une organisation qui ne respecte pas les prescriptions relatives à la sécurité de l'information. Cette loi peut comporter des articles qui définissent la gravité de certains types de violations de la confidentialité ou d'autres aspects des informations et les sanctions correspondantes.

3.7. Le pouvoir réglementaire des autorités compétentes devrait leur permettre d'imposer des obligations aux détenteurs d'informations sensibles. Les lois adoptées à cet effet devraient prévoir des sanctions ou des peines en cas de divulgation non autorisée. La législation devrait également imposer que les ministères, directions, organes et autres organisations de l'État apportent aux autorités compétentes tout le soutien nécessaire pour leur permettre d'assurer la sécurité des informations sensibles.

ÉLABORATION DES ORIENTATIONS NATIONALES

3.8. La politique de l'État relative à la sécurité devrait définir les types d'informations que l'État souhaite sécuriser et indiquer comment cette sécurité doit être assurée. Cet élément figure généralement dans un manuel de sécurité établi par les autorités nationales de sécurité (ou par une autre autorité appropriée). Un tel manuel peut ne pas faire directement référence aux informations sensibles pour la sécurité nucléaire. Il définit cependant les différentes catégories d'informations en indiquant leur niveau de sensibilité et donc le niveau de sécurité à appliquer et précise comment les objets informationnels devraient être marqués afin que leur niveau de sensibilité apparaisse clairement.

3.9. Des orientations détaillées sur les informations qui peuvent être qualifiées de sensibles devraient être fournies par les autorités compétentes concernées, en liaison étroite avec les autorités nationales de sécurité et avec la participation d'utilisateurs de matières nucléaires ou d'autres matières radioactives. Ces

orientations se fondent le plus souvent sur les conclusions d'une évaluation nationale de la menace et devraient être conformes à celles-ci. Parfois appelées règles de classification, elles répartissent généralement les types d'informations suivant le thème auquel elles se rapportent et indiquent l'importance relative d'une information particulière et donc sa sensibilité et le degré de sécurité à appliquer.

3.10. Au niveau d'une organisation, l'importance d'informations particulières peut figurer dans son plan de sécurité, lequel devrait décrire comment chaque type d'information sensible doit être protégé conformément à la législation et à la réglementation nationales.

POLITIQUES DE SÉCURITÉ

3.11. En plus de la publication de politiques de sécurité de l'information conformes aux prescriptions nationales, les autorités compétentes devraient donner des informations détaillées sur la façon dont ces prescriptions devraient être appliquées aux installations et aux activités qui mettent en jeu des matières nucléaires ou d'autres matières radioactives.

3.12. La politique nationale de sécurité devrait montrer un engagement en faveur de la sécurité de l'information. Elle devrait se traduire par la publication et le maintien d'une politique de sécurité de l'information complète et appropriée à appliquer dans toutes les installations et activités mettant en jeu des matières nucléaires ou d'autres matières radioactives, ainsi que dans tous les autres lieux où des informations sensibles connexes sont conservées. Le but de cette politique est de garantir que les informations sensibles ne puissent faire l'objet d'une compromission.

3.13. Chaque organisation et chaque installation qui exploite des informations sensibles devrait ensuite établir sa propre politique de sécurité de l'information, à partir de celle qui a été élaborée par les autorités s'il y a lieu. Cette politique devrait être communiquée à toute l'organisation sous une forme appropriée, accessible et compréhensible pour les utilisateurs auxquels elle s'adresse. La section 6 contient des orientations supplémentaires concernant l'instauration d'un programme de gestion de la sécurité de l'information, y compris sur la question de la définition des politiques dans ce domaine.

SYSTÈMES DE CLASSIFICATION DES INFORMATIONS

3.14. Pour mettre en œuvre un système de sécurité de l'information et effectuer les contrôles correspondants, il faut des moyens et du temps. Il n'est ni possible ni souhaitable de sécuriser de la même manière toutes les informations au niveau d'un site ou d'une installation. Certaines informations ne sont pas sensibles et ne nécessitent pas de mesures de protections particulières. Même pour ce qui est des informations sensibles, les divers objets informationnels n'appellent pas tous le même niveau de sécurité. Il importe donc de déterminer quelles sont les informations sensibles et quel degré de sécurité elles réclament. Dans chaque État, les autorités compétentes devraient décider quelles informations relatives aux matières nucléaires, aux autres matières radioactives et aux installations et activités associées constituent des informations sensibles. En matière de transport international, chaque État devrait déterminer les informations à protéger et voudra peut-être se pencher sur la cohérence des pratiques entre les États concernés par le transport international.

3.15. La méthode recommandée pour évaluer un actif informationnel particulier consiste à suivre une démarche fondée sur la connaissance des risques en tenant compte des dommages et des conséquences qui sont susceptibles de se produire en cas de compromission de l'actif concerné. Il importe de noter que la compromission d'une information quelconque au niveau d'une installation peut avoir des répercussions sur d'autres installations détenant des actifs informationnels semblables. Les dommages et les conséquences devraient donc être envisagés de manière globale afin de prendre en considération les effets sur la sécurité nucléaire dans d'autres endroits et pas uniquement dans un lieu donné. Une attention particulière devrait être accordée aux concentrations d'informations et aux points de défaillance uniques possibles (par exemple, des actifs informationnels qui dépendent d'un seul réseau ou ne disposent que d'une seule source d'alimentation électrique). Les résultats de l'évaluation peuvent servir à déterminer le niveau de sécurité nécessaire pour chaque objet informationnel conformément au système de classification adopté par l'État concerné.

3.16. Un système de classification national devrait être établi et tenu à jour afin de regrouper les informations par catégorie, de telle sorte que les informations dont la divulgation non autorisée aurait des conséquences similaires soient classées dans la même catégorie et que, par conséquent, les informations d'une même catégorie fassent l'objet de prescriptions semblables en matière de sécurité. Il devrait s'agir d'un système national et non d'un système limité à un secteur particulier ou conçu par une seule installation. Très souvent, les États gèrent de

tels systèmes de classification, mais ceux-ci ne prennent pas toujours en compte les informations propres à la sécurité nucléaire. Ce type de système repose sur une démarche fondée sur la connaissance des risques, dans laquelle les conséquences possibles de la divulgation non autorisée d'informations déterminent la catégorie et les prescriptions de sécurité qui s'appliquent à celles-ci.

3.17. Il conviendrait d'examiner avec soin la question du nombre de catégories de la classification et des bénéfices que l'on peut tirer de leur utilisation. Un système très complexe peut être pesant et se révéler peu pratique, tandis que la classification ne sera peut-être pas assez précise avec un système très simple. De plus, il conviendrait de faire preuve de discernement dans l'attribution d'un niveau de classification à un objet informationnel. Une surclassification (c'est-à-dire le fait d'imposer des conditions de sécurité plus rigoureuses que ce qui est réellement nécessaire) peut donner lieu à des dépenses supplémentaires inutiles, tandis qu'une sous-classsification peut exposer les informations à un risque de compromission inacceptable. Une surclassification peut aussi être en conflit avec les politiques de transparence ou conduire les personnes qui utilisent les informations à considérer que la classification est peu pertinente.

3.18. Un système de classification possible pour les informations sensibles, où les catégories indiquent la sensibilité d'objets informationnels particuliers, pourrait comporter les niveaux suivants[1] :

a) SECRET ;
b) CONFIDENTIEL ;
c) RESTREINT.

3.19. Des mentions supplémentaires peuvent signaler les restrictions à la diffusion d'une information qui résultent de la classification de l'information concernée, notamment :

a) aucune distribution supplémentaire ;
b) distribution contrôlée par l'entité qui est à l'origine de l'information ;
c) à usage officiel ;
d) distribution restreinte ;
e) accessible pour le public.

---

[1] Dans de nombreux États, il existe aussi une catégorie TRÈS SECRET, qui n'est pratiquement jamais utilisée dans le secteur civil de la plupart des pays. Elle sert généralement dans le secteur militaire et dans celui de l'armement.

3.20. On trouvera dans l'annexe I des exemples de définition pour les niveaux de classification SECRET à RESTREINT.

4. DÉTERMINATION DES INFORMATIONS SENSIBLES

4.1. En matière de classification et de protection des informations, la première étape consiste à déterminer les informations considérées comme sensibles.

4.2. Des mesures de sécurité devraient au moins être envisagées pour les informations qui appartiennent aux catégories suivantes, susceptibles d'avoir une incidence sur la sécurité nucléaire[2] :

a) renseignements détaillés sur les systèmes de protection physique et sur toutes les autres mesures de sécurité en vigueur pour les matières nucléaires, les autres matières radioactives et les installations et activités associées, y compris les informations sur les agents de sécurité et les forces d'intervention ;
b) informations relatives à la quantité et à la forme des matières nucléaires ou d'autres matières radioactives utilisées ou entreposées, y compris les informations concernant la comptabilité des matières nucléaires ;
c) informations relatives à la quantité et à la forme de matières nucléaires ou d'autres matières radioactives transportées ;
d) renseignements détaillés sur les systèmes informatiques, y compris les systèmes de communication, qui traitent, exploitent, stockent ou transmettent des informations ayant directement ou indirectement de l'importance pour la sûreté et la sécurité ;
e) plans d'urgence et d'intervention en cas d'événement de sécurité nucléaire ;
f) données personnelles sur les salariés, les vendeurs et les entreprises extérieures ;
g) évaluations de la menace et critères appliqués pour déclencher des alertes sur la sécurité ;
h) renseignements détaillés sur des technologies sensibles ;

[2] Cette liste ne prévoit pas toutes les possibilités, mais devrait servir de point de départ à la réflexion.

i) informations détaillées sur des vulnérabilités ou des faiblesses qui concernent les sujets mentionnés ci-dessus ;

j) données historiques sur l'un quelconque des sujets mentionnés ci-dessus.

Certaines des informations citées ci-dessus, comme les données personnelles, peuvent aussi faire l'objet de prescriptions de sécurité particulières en application d'autres lois nationales ou d'une politique d'entreprise.

4.3. L'annexe II présente des exemples de types particuliers d'informations appartenant aux catégories énumérées au paragraphe 4.2 en indiquant si elles sont généralement considérées comme sensibles et pour quelle raison.

5. MISE EN COMMUN ET DIVULGATION D'INFORMATIONS SENSIBLES

5.1. Il est souvent nécessaire de mettre en commun des informations sensibles de manière régulière, par exemple entre organismes nationaux compétents, entre les organisations qui manipulent des matières nucléaires ou d'autres matières radioactives et les autorités compétentes concernées ou entre différents États. De même, il est parfois indispensable de divulguer des informations sensibles de façon ponctuelle à d'autres organisations ou au public. La mise en commun et la divulgation devraient être gérées de telle sorte que les informations sensibles ne soient pas communiquées à des personnes qui n'ont pas besoin de les connaître.

MISE EN COMMUN D'INFORMATIONS

5.2. Il est parfois nécessaire de mettre certaines informations sensibles à la disposition des organismes nationaux autorisés ou des entreprises ou organisations ayant besoin de les connaître. La mise en commun d'informations permet parfois d'obtenir des gains d'efficacité qui n'existeraient pas si les informations devaient être produites et exploitées indépendamment les unes des autres. Le fait de ne pas mettre à disposition des informations peut parfois aussi nuire à la sécurité ou à la planification, à la conception et à la mise en œuvre de mesures de sécurité. En outre, assez souvent, les responsabilités relatives à la sécurité nucléaire ne relèvent pas d'un seul organisme, d'une seule entreprise ou d'une seule organisation. Des informations doivent donc souvent être mises en commun

entre ceux qui partagent les responsabilités en matière de sécurité. Dans l'intérêt de la sécurité nationale, les autorités compétentes sont ainsi souvent amenées à transmettre des informations sensibles aux autorités nationales de sécurité et vice-versa. Les modifications apportées à une évaluation de la menace ou des informations sur un événement lié à la sécurité devraient être communiquées aux acteurs intéressés en temps opportun afin d'ajuster les mesures de sécurité, de mettre en commun les expériences d'exploitation et de contribuer ainsi à l'amélioration continue en la matière. Indépendamment des questions de sécurité, la mise à disposition d'informations peut être nécessaires dans d'autres domaines comme les évaluations de la sûreté et les besoins opérationnels ou commerciaux.

5.3. La nature et l'ampleur de la mise en commun de ces informations doivent d'abord être conformes à la législation et à la réglementation nationales et ensuite assurer un équilibre entre les avantages de la mise en commun et les besoins de la sécurité. La transmission d'informations entre autorités devrait être régie par les procédures de sécurité en vigueur dans l'État concerné. L'instauration d'une approche commune au sein d'un État peut garantir que des informations sensibles ne soient pas divulguées inopportunément.

5.4. Souvent, il est également nécessaire de mettre certaines informations à la disposition d'autres États ou d'organisations internationales concernées. En pareil cas, un accord devrait être en vigueur afin de garantir que les informations sensibles seront protégées par le destinataire conformément aux prescriptions du propriétaire des informations. La sécurité de l'information peut être assurée par un traité ou un accord bilatéral ou multilatéral qui détermine comment les informations seront protégées contre la divulgation. Ces accords décrivent généralement les mesures de protection à appliquer aux informations sensibles pour les différents niveaux de classification dans chaque État. Ils devraient également tenir compte de la façon dont des prescriptions particulières en vigueur dans un des États (par exemple, la législation relative à la liberté d'information, voir le paragraphe 5.6) pourraient avoir des répercussions sur l'exploitation des informations sensibles d'autres États.

DIVULGATION D'INFORMATIONS

Besoin de divulgation

5.5. La plupart des États disposent d'une loi sur la sécurité des informations d'intérêt national. Ce type de loi précise les sanctions encourues par un ressortissant de l'État concerné ou une autre personne qui enfreindrait la législation

relative à la confidentialité des informations de cette nature. En général, il existe aussi des lois qui réglementent l'accès des individus aux informations officielles émanant de l'État. Des mécanismes de règlement des différends entre l'État et d'autres acteurs au sujet des informations qui ne doivent pas être divulguées afin de protéger la sécurité nationale ont également été adoptés.

5.6. Plusieurs États disposent d'une législation sur la liberté d'information ou d'autres lois qui permettent aux personnes du public de demander à consulter des informations détenues par les autorités. En règle générale, les seules informations que les autorités peuvent refuser de divulguer sont celles qui bénéficient d'exemptions précises, comme les informations liées à la défense nationale ou les informations privées et personnelles. Dans plusieurs États, un élément qui porte une marque de classification n'est pas automatiquement soustrait à la divulgation.

5.7. D'autres lois et règlements peuvent disposer que certains types d'informations, qui peuvent comprendre des informations sensibles, soient divulguées. On peut citer par exemple la législation environnementale, qui impose de communiquer certaines informations au public. Il conviendrait que ce type de loi permette de soustraire à la divulgation les informations qui pourraient avoir une incidence sur la sécurité nationale ou sur la sécurité de tiers.

Élaboration d'orientations sur la divulgation

5.8. Des orientations spécifiques devraient être élaborées afin d'aider les organisations et les installations à déterminer quelles sont les informations sensibles qui peuvent être divulguées. Lors de la rédaction de ces orientations, l'organisme public responsable consulte généralement d'autres services gouvernementaux et des organisations compétentes. En déterminant le type d'informations qu'il n'est pas jugé souhaitable de divulguer, les orientations devraient contribuer à prévenir la divulgation non autorisée d'informations sensibles (voir également l'annexe II).

5.9. Les États devraient envisager de fournir des orientations spécifiques sur :

a) la sensibilité de certains types d'informations sensibles en fonction des conséquences de leur divulgation ;
b) les types d'informations qui peuvent être divulguées, dans quelles circonstances, à qui et de quelle manière particulière ;
c) les conditions de la divulgation des informations ;
d) les procédures de passage en revue des informations afin d'en déterminer l'éventuelle sensibilité avant qu'elles ne soient rendues publiques, par

exemple dans le cadre d'une conférence, sous forme de publications sur le web ou dans des spécifications techniques ;

e) les mesures qu'il conviendrait de prendre en cas de divulgation non autorisée d'informations sensibles, que la divulgation ait été délibérée ou involontaire, ou d'une autre violation des prescriptions relatives à la sécurité de l'information.

5.10. Les orientations devront être modifiables. En effet, les circonstances évoluent et des informations qui pouvaient être considérées comme sensibles et dont la divulgation n'était pas jugée souhaitable à un moment donné peuvent devenir beaucoup moins sensibles et leur divulgation appropriée ultérieurement (et vice-versa). Il conviendrait donc de réexaminer et d'actualiser les orientations de manière périodique et en cas de changement important de politique ou de circonstances.

5.11. Il est généralement possible d'abaisser le niveau de sécurité qui s'applique à des informations particulières lorsqu'il y a lieu. En revanche, faire passer une information dans une catégorie plus confidentielle peut être impossible ou sans effet si elle a déjà été plus largement divulguée. Ce point devrait être pris en compte lors de la classification initiale et il conviendrait de trouver un équilibre approprié entre confidentialité et prudence, d'une part, et disponibilité et transparence, d'autre part. Il conviendrait d'établir un calendrier de référence pour le réexamen périodique des classifications, sachant que des changements devraient également être apportés chaque fois que nécessaire, par exemple lorsque les circonstances évoluent sensiblement.

5.12. Toutes les demandes de divulgation d'informations sensibles adressées à une organisation devraient être examinées au regard des mêmes orientations ou des mêmes critères et, lorsque cela est possible, devraient être traitées par un seul bureau central pour toute l'organisation. Pour accéder à des informations sensibles de manière répréhensible, l'une des techniques possibles, couramment utilisée, consiste à adresser de multiples demandes à divers individus ou à différents services au sein d'une même organisation. Si ces demandes sont traitées séparément et sans coordination, des réponses différentes risquent d'être données et des informations sensibles qui, en d'autres circonstances, n'auraient pas été divulguées, risquent de l'être.

6. CADRE DE GESTION DE LA CONFIDENTIALITÉ

6.1. La section 3 décrit le cadre général de protection des informations sensibles. La présente section examine plus en détail les éléments de ce cadre qui sont nécessaires dans une installation ou une organisation, en les étudiant dans la perspective du système de gestion.

6.2. Un système de gestion établissant les politiques et les objectifs et permettant d'atteindre ces derniers de manière efficiente et efficace devrait être mis en place. Un système intégré de gestion (voir le nº GS-R-3 de la collection Normes de sûreté de l'AIEA, intitulé *Système de gestion des installations et des activités* [8] et les orientations qui y sont associées) constitue un élément essentiel de l'appui à une culture de sécurité nucléaire. Dans les installations, de nombreuses activités sont contrôlées par des systèmes de gestion. Dans l'idéal, ces derniers intègrent des éléments relatifs à la sécurité, à la sûreté, à la santé, à l'environnement, à la qualité et à l'économie dans un mécanisme de gestion unique ou dans un ensemble de systèmes intégrés et synergiques. La sécurité de l'information devrait être intégrée au système de gestion de l'installation ou de l'organisation afin d'assurer la confidentialité, l'intégrité et la disponibilité des informations.

6.3. Pour assurer la confidentialité, l'intégrité et la disponibilité des informations sensibles, il faut définir le rôle et les responsabilités de chacun, disposer d'une classification permettant de déterminer quelles informations sont sensibles et doivent être protégées, pour quelle raison et à quel niveau (voir la section 4), prendre des décisions quant à la manière de protéger ces informations, mettre en œuvre les mesures de sécurité nécessaires et procéder à une intervention (comprenant une récupération) au cas où ces informations seraient compromises, volées ou perdues.

6.4. Le cadre de gestion présenté ci-après s'applique à tous les niveaux de décision dans les organisations qui détiennent ou exploitent des informations sensibles.

RESPONSABILITÉS

6.5. La direction a la responsabilité générale de veiller à ce qu'un dispositif de sécurité de l'information soit en place et effectif dans toute l'installation ou l'organisation afin de protéger les informations sensibles. Tous les membres du

personnel qui exploitent des informations sensibles ont la responsabilité d'assurer leur sécurité conformément à la législation nationale applicable et aux politiques et procédures de l'organisation.

Responsabilités de la direction

6.6. Exemples de responsabilités qui incombent généralement à la direction :

a) assumer la responsabilité générale de la protection des informations sensibles et des ressources d'informations sensibles ;
b) s'assurer du respect des lois et des règlements applicables ;
c) attribuer les responsabilités organisationnelles en matière de sécurité ;
d) organiser des formations théoriques et pratiques efficaces dans le domaine de la sécurité ;
e) veiller à la mise en place d'une politique de sécurité de l'information efficace ;
f) fournir des ressources adéquates pour la mise en œuvre d'un programme de sécurité de l'information efficace ;
g) veiller au développement du programme de sécurité de l'information et des plans et procédures qui y sont associés ;
h) assurer une gestion du changement efficace concernant les plans, les procédures et les politiques ;
i) veiller à ce que la politique et les procédures de sécurité de l'information fassent régulièrement l'objet d'audits, de réexamens et de révisions.

Responsabilités en matière de classification

6.7. Les autorités compétentes devraient fournir des orientations sur la catégorie dont fait partie un objet informationnel sous la forme d'un guide ou d'orientations de classification. Ce type de documents regroupe les informations autour de thèmes particuliers et indique la sensibilité des informations. Les entités qui sont à l'origine d'informations sensibles devraient se servir d'un guide de cette nature lorsqu'ils déterminent le niveau de classification à appliquer à une information.

6.8. Une fois les informations diffusées, le destinataire ou le détenteur d'un objet informationnel sensible ne devrait pas modifier le niveau de classification qui a été appliqué à ces informations sans l'autorisation de l'entité qui en est à l'origine. Les destinataires et les détenteurs des textes peuvent et, lorsqu'il y a lieu, devraient contester le niveau de classification qui a été appliqué. Par exemple, si l'autorité compétente recevait d'un exploitant des informations

dont la catégorie est erronée au regard de la législation applicable, elle devrait ordonner à l'exploitant de classer ces informations dans la bonne catégorie.

6.9. Si l'organisation qui est à l'origine des informations cesse ses activités, l'organisation qui lui succède devient responsable. S'il n'est pas possible de déterminer quelle est cette organisation, le détenteur d'un objet informationnel sensible peut, s'il y a lieu, classer cet objet dans une autre catégorie après consultation des autorités compétentes concernées.

6.10. Si le niveau de classification appliqué à un objet informationnel ou à un type d'objet informationnel est modifié, cette modification devrait être signalée à toutes les personnes susceptibles d'en subir les conséquences dans la mesure du possible. Cette liste de personnes peut comprendre les détenteurs passés et actuels des informations en question, ainsi que ceux qui pourraient s'en servir à l'avenir.

PLAN DE SÉCURITÉ

6.11. Toutes les organisations qui exploitent des informations sensibles devraient mettre en place un plan de sécurité. Ce plan devrait comporter une partie détaillée portant spécifiquement sur la sécurité des informations sensibles. Les prescriptions appropriées du plan de sécurité devraient être communiquées aux salariés et aux entreprises extérieures qui travaillent pour l'organisation concernée. Il est indispensable que les salariés et les entreprises extérieures connaissent leurs responsabilités.

POLITIQUE ET PROCÉDURES DE SÉCURITÉ

Plan de sécurité de l'information

6.12. Les responsabilités relatives à la sécurité de l'information devraient être décrites dans les politiques et procédures de chaque organisation. Au minimum, les points suivants devraient être abordés :

a) définition de la sécurité de l'information et énoncé des objectifs généraux, du périmètre et de l'importance de cette activité ;
b) définition du rôle et des responsabilités des différents acteurs, comprenant la désignation d'un coordonnateur chargé de diriger et d'administrer la sécurité ;

c) respect des prescriptions relatives à la sécurité de l'information, notamment les prescriptions législatives, réglementaires et contractuelles ;
d) élaboration d'un plan de gestion des risques visant à ramener les risques à un niveau acceptable et défini par l'État grâce des contrôles adéquats déterminés par l'évaluation des risques. Pour une installation nucléaire, ce plan devrait être approuvé par l'autorité compétente ou par une autre autorité désignée par l'État à cette fin ;
e) contrôle et réexamen réguliers des dispositions en vigueur afin de s'assurer que la politique, les normes et les procédures qui sont appliquées restent pertinentes et efficaces ;
f) prescriptions relatives à la formation théorique et pratique afin que le personnel, les entreprises extérieures et les autres intervenants aient connaissance de la politique, des procédures et des dispositions pratiques en vigueur suivant les besoins de leurs fonctions et aient parfaitement conscience de leurs responsabilités (y compris leurs obligations juridiques) ;
g) conséquences (peines ou sanctions) en cas de non-respect des prescriptions relatives à la sécurité de l'information ou de négligence délibérée concernant la protection d'informations sensibles ;
h) documentation de référence à l'appui de la politique en vigueur, par exemple des procédures plus détaillées concernant des systèmes particuliers ou des règles de sécurité que les utilisateurs devraient observer.

Aspects du plan de sécurité de l'information qui concernent spécifiquement les informations sensibles

6.13. S'agissant particulièrement de la protection des informations sensibles, le plan devrait également aborder les points suivants :

a) cycle de vie de l'information : définition des procédures à suivre pour produire, recenser, classer, marquer, exploiter, utiliser, stocker, transmettre, reclasser, reproduire et détruire des informations sensibles ;
b) prescriptions de sécurité applicables aux informations sensibles, en tenant dûment compte des objectifs de la sécurité que sont la confidentialité, l'intégrité et la disponibilité des informations ;
c) accès aux informations sensibles et aux ressources d'informations sensibles limité aux personnes qui ont besoin d'y accéder pour remplir leurs fonctions, qui disposent des pouvoirs nécessaires et qui ont été soumises à un contrôle de fiabilité adapté au niveau de classification des informations concernées ;

d) transmission d'informations sensibles d'une manière qui ramène le risque de compromission, d'interception non autorisée, de modification et de perturbation à un niveau acceptable.

Procédures relatives à l'exploitation des informations sensibles

6.14. Pour gérer efficacement les risques liés aux menaces qui pèsent sur la confidentialité, l'intégrité et la disponibilité des informations, il faut mettre au point des contre-mesures efficaces permettant de parer à ces menaces. Ces mécanismes se traduisent nécessairement par des mesures de sécurité concernant la sécurité de l'information, la protection physique et les habilitations de sécurité.

6.15. Les habilitations de sécurité, contrôles de fiabilité inclus, garantissent que les personnes qui ont accès à des informations sensibles sont considérées par l'État comme suffisamment fiables pour y avoir accès. S'agissant des informations dont le niveau de classification est relativement bas, l'organisation devrait décider s'il est nécessaire ou non de contrôler les personnes qui ont besoin d'y accéder. Dans l'affirmative, un contrôle limité du parcours de l'individu concerné peut être suffisant. En ce qui concerne l'accès aux informations dont le niveau de classification est plus élevé, il faut effectuer une série plus complète de contrôles des antécédents pour pouvoir déterminer la fiabilité d'un individu. Les habilitations de sécurité devraient également prévoir la signature d'un accord de confidentialité entre la personne et l'autorité compétente ou l'organisation concernée.

6.16. La protection physique associe souvent un accès strictement réglementé à un périmètre sécurisé et un ou plusieurs dispositifs de protection physique supplémentaires autour des actifs informationnels, par exemple une chambre forte ou un autre type de lieu sûr. Les mêmes principes peuvent être appliqués pour assurer la protection physique des informations et des actifs informationnels.

6.17. Les mesures relatives à la sécurité de l'information intègrent des contrôles techniques, opérationnels et administratifs qui sont appliqués à toutes les étapes de la vie d'un objet informationnel : création, exploitation, stockage, transmission, reproduction et destruction. Elles comprennent notamment les dispositions suivantes :

a) gestion administrative destinée à régir, maintenir et renforcer la sécurité de l'information (y compris pour les services fournis par des tiers) ;
b) mesures relatives à la fiabilité du personnel, en particulier pendant le recrutement et au début et à la fin d'un emploi ;

c) sécurité physique des lieux où se trouvent des informations sensibles ou des ressources d'informations sensibles et des lieux où elles sont utilisées ou traitées ;
d) sécurité du traitement numérique ou manuel des informations : sécurité du poste de travail, protection contre les virus et les logiciels malveillants, effacement et destruction des informations, opérations manuelles ;
e) sécurité des réseaux de télécommunications (téléphones, courriels, Internet et réseaux locaux) : politique, authentification des utilisateurs, identification des équipements, séparation des responsabilités, contrôles des connexions et de l'acheminement, et surveillance ;
f) sécurité du matériel : contrôle d'accès, journalisation de l'activité des utilisateurs et des administrateurs, gestion des pièces détachées, matériel critique de secours, alimentations de secours, documentation et maintenance, sécurité du câblage et des supports électroniques ;
g) sécurité logicielle : contrôle d'accès, journalisation de l'activité des utilisateurs et des administrateurs, gestion des sauvegardes, contrats de maintenance, configuration et gestion des versions, utilisation de logiciels autorisés, tests de vulnérabilité et tests du comportement du système en cas d'erreur ;
h) sécurité d'utilisation des systèmes d'information : contrôle des droits utilisateur, identification de l'utilisateur et vérification de son identité, connexion aux services, aux systèmes et aux appareils, gestion des mots de passe, surveillance de l'utilisation, règle des deux personnes (c'est-à-dire contrôle par deux personnes) pour les opérations les plus délicates ;
i) classification et procédures correspondantes pour l'exploitation des informations ;
j) protection de la vie privée.

6.18. L'exploitation des informations sensibles devrait être régie par des procédures conformes à la partie relative à la sécurité de l'information de la politique et des orientations de sécurité nationale, ainsi qu'à toute interprétation qu'en donnent les autorités compétentes de l'État concerné. Les exigences de performance minimales pour les différents niveaux de sécurité devraient être décrites dans le plan de sécurité de l'information. À titre d'exemple, on peut citer la méthode de cryptage utilisée pour la transmission électronique des informations.

Système de gestion des droits

6.19. Il conviendrait de mettre en place un système de gestion qui contrôle comment, pourquoi et quand des détenteurs et des utilisateurs particuliers

d'informations sensibles devraient être autorisés à accéder aux informations sensibles et aux ressources d'informations sensibles. Un système de gestion des droits comprend généralement :

a) une structure de responsabilité pour la gestion des autorisations ;
b) des procédures pour déterminer qui a le droit de nommer qui et qui a le droit d'accéder aux informations sensibles et aux ressources d'informations sensibles ;
c) des procédures pour savoir comment vérifier, contrôler et superviser l'attribution des droits d'accès ;
d) des procédures pour déterminer combien de temps une autorisation d'accès à des informations sensibles et à des ressources d'informations sensibles devrait être valide ;
e) des procédures pour abroger une autorisation d'accès à des informations sensibles et à des ressources d'informations sensibles ;
f) des procédures permettant d'assurer une traçabilité sans faille pour la gestion des droits à toutes les étapes de la chaîne de décision pour les autorisations d'accès aux informations sensibles et aux ressources d'informations sensibles.

Réexamens périodiques

6.20. Les politiques, les plans et les procédures de sécurité devraient évoluer en fonction des circonstances. Pour s'assurer qu'ils seront maintenus à jour, une méthode efficace consiste à inclure un calendrier de réexamen dans les documents eux-mêmes. En cas de changement de circonstances fondamental pouvant se traduire par une modification de la politique adoptée, par exemple une évolution législative, un réexamen peut avoir lieu avant l'échéance prévue. Le réexamen devrait porter sur la politique applicable à tous les niveaux de responsabilité ayant trait à la sécurité nucléaire.

CULTURE DE SÉCURITÉ

6.21. L'élaboration, la promotion et le maintien d'une solide culture de sécurité nucléaire constituent un élément essentiel d'un régime de sécurité nucléaire et en particulier en matière de sécurité de l'information, pour laquelle les hommes et les procédures jouent souvent un rôle déterminant dans la protection des informations.

6.22. Dans le cadre d'une véritable culture de sécurité nucléaire [9], toutes les organisations, tous les salariés et toutes les entreprises extérieures devraient parfaitement connaître leurs responsabilités en matière de sécurité et l'importance de ces responsabilités. Dans ce domaine, il est indispensable que les salariés et les membres des entreprises extérieures reçoivent une formation théorique et pratique en adéquation avec leurs responsabilités et leurs besoins.

6.23. Les salariés et les membres des entreprises extérieures qui exercent des responsabilités particulières en matière de sécurité ou qui ont accès à des informations sensibles, ainsi que l'encadrement à tous les niveaux d'une organisation, ont besoin d'une formation et de séances d'information spécifiques sur leurs responsabilités. Il importe aussi de veiller à ce que d'autres catégories de salariés (comme les coursiers, le personnel de sécurité et les employés de bureau) qui traitent des informations sensibles sans nécessairement connaître leur contenu reçoivent également une formation sur la sécurité adaptée à leurs responsabilités.

6.24. Les formations ponctuelles sur la sécurité de l'information ne permettent pas de consolider les connaissances et, à long terme, peuvent rendre les salariés trop confiants. Toutes les personnes qui gèrent des informations sensibles, notamment tous les cadres, tous les salariés et tous les membres d'entreprises extérieures, devraient recevoir une formation continue en cours d'emploi et assister régulièrement à des cours de recyclage. Il conviendrait de garder une trace des formations structurées qui ont été suivies jusqu'à leur terme par tous les salariés et tous les membres d'entreprises extérieures. Il importe en particulier que toute modification des règles et procédures de sécurité soit portée dès que possible à la connaissance de tous les salariés et de tous les membres d'entreprises extérieures concernés. On trouvera en annexe III une proposition de cadre et de contenu pour un programme de formation et de sensibilisation.

ACCORDS AVEC DES TIERS SUR LA SÉCURITÉ DE L'INFORMATION

6.25. Une autorité compétente ou une organisation a parfois besoin qu'un tiers lui fournisse des services ou des biens mettant en jeu des informations sensibles. Dans ce cas, elle devrait conclure une convention, par exemple une licence ou un contrat, et un accord de confidentialité. Lorsqu'un tel accord est conclu avec un tiers, il arrive que des informations sensibles lui soient confiées. Afin que ces informations ne soient pas compromises, il devrait exister une politique ou une loi portant sur les accords qui mettent en jeu des informations sensibles.

Les organisations et les installations contractantes devraient alors être tenues de suivre cette politique.

6.26. Lorsqu'elles négocient avec des tiers en vue d'établir des relations, les organisations contractantes doivent veiller à ce que toutes les informations sensibles qui seront confiées à des tiers soient convenablement protégées. Les mesures de sécurité mises en place pour protéger les informations sensibles devraient être adaptées aux risques encourus et conformes à la politique en vigueur.

6.27. Dans ce cadre, les autorités compétentes et les organisations devraient s'assurer que les tiers :

a) ont mis en place des méthodes et des procédures de sécurité qui satisfont au moins aux propres prescriptions de l'organisation en matière de sécurité ;
b) ont désigné un coordonnateur pour diriger et gérer la sécurité au niveau de l'entreprise contractante ;
c) ont mis en place un mécanisme afin que tous les membres du personnel ayant accès à des informations sensibles détenues par des tiers soient soumis à un contrôle de fiabilité approprié ;
d) veillent à ce que l'accès aux informations sensibles et aux ressources d'informations sensibles soit exclusivement limité aux personnes qui ont absolument besoin de les connaître et qui disposent de l'habilitation de sécurité appropriée ;
e) transmettent les informations conformément à la législation nationale et à la politique de l'organisation et de telle manière qu'elles ne risquent pas d'être compromises ;
f) veillent à ce que des informations ne soient pas mises à la disposition d'une entité ou d'un individu non autorisés ;
g) veillent à ce que tout leur personnel ait connaissance de la politique et des dispositions pratiques en matière de sécurité et ait parfaitement conscience de ses responsabilités (y compris de ses obligations juridiques) ;
h) disposent de procédures pour faire face aux événements liés à la sécurité de l'information ;
i) veillent à ce que les mesures de sécurité en vigueur dans leurs locaux soient régulièrement contrôlées par les autorités compétentes ou par les organisations contractantes en application des dispositions de l'accord afin de vérifier qu'elles sont conformes aux prescriptions de l'accord en matière de sécurité.

INSPECTIONS ET AUDITS

6.28. Pour un programme de sécurité de l'information, la réalisation régulière d'activités de contrôle est indispensable. Il faut avoir l'assurance que les programmes de sécurité mis en place dans les organisations qui détiennent des informations sensibles et chez les tiers satisfont en tous points à la politique et aux règlements nationaux. Les mesures relatives à la sécurité de l'information devraient si possible être contrôlées par les autorités compétentes avant que celles-ci ne donnent officiellement leur accord pour qu'elles soient appliquées. Le contrôle peut prendre la forme d'inspections ou d'audits réguliers et officiels de l'organisation ou de l'installation. Un audit est généralement effectué en interne, tandis qu'une inspection peut être réalisée aussi bien en interne qu'en externe. De plus, une inspection peut être annoncée, mais elle peut aussi être inopinée (en d'autres termes, elle peut avoir lieu avec ou sans préavis).

6.29. Une organisation réalise des inspections et des audits internes pour déterminer si le programme de sécurité mis en place est conforme au plan de sécurité de l'information qui a été approuvé et pour vérifier que les prescriptions réglementaires sont bien respectées. Ces démarches permettent à une organisation de procéder à un contrôle plus souvent qu'avec des inspections externes. De plus, les inspections et les audits menés par des membres du personnel qui connaissent bien les prescriptions, les procédures et les mécanismes internes peuvent mettre en évidence des possibilités d'amélioration différentes de celles qui pourraient être découvertes lors d'une inspection externe.

6.30. Les inspections externes sont menées par les autorités compétentes ou par un autre organisme extérieur habilité à cette fin. Le but de ces inspections est d'évaluer le niveau de conformité par rapport à la politique nationale de sécurité de l'information. Une inspection externe constitue une évaluation indépendante, contrairement à une inspection réalisée par l'organisation elle-même. Lorsque des auditeurs externes interviennent, les questions de confidentialité et de fiabilité devraient être traitées.

6.31. Les conclusions d'une inspection ou d'un audit devraient mettre en lumière les secteurs spécifiques dans lesquels il faut agir ou apporter des améliorations. Les actions préventives ou correctrices recensées devraient être associées à un calendrier spécifique de mise en œuvre. Ces actions devraient faire l'objet d'un suivi et leur efficacité devrait être évaluée.

INCIDENTS LIÉS À LA SÉCURITÉ DE L'INFORMATION

6.32. Les atteintes à la sécurité peuvent être dues à la compromission d'un objet informationnel. Les fuites et les pertes constituent deux types d'atteintes dans lesquels une information est compromise. Une fuite correspond généralement à une confidentialité compromise par suite de la divulgation non autorisée d'une information de manière accidentelle ou délibérée. Une perte correspond généralement à une information compromise par suite du vol ou de la mauvaise protection d'une information ou d'actifs informationnels.

6.33. Les incidents liés à la sécurité de l'information comprennent également les pertes de disponibilité ou d'intégrité d'une information, qui peuvent être involontaires ou intentionnelles. Une perte de disponibilité peut par exemple être due à une anomalie dans un système d'information (une base de données, par exemple) ou à un refus d'utilisation malveillant (perturbation intentionnelle d'un réseau d'information par génération d'un trafic de données excessif). Une perte d'intégrité peut par exemple être due à un dommage subi par un système d'information, à la corruption d'une base de données ou à la transformation non autorisée d'informations au cours de leur transmission.

6.34. Le signalement aux autorités compétentes des atteintes ou des incidents importants en matière de sécurité nucléaire, y compris les atteintes à la sécurité de l'information, devrait être obligatoire et cette prescription devrait figurer dans la législation ou la réglementation nationales. La législation ou la réglementation devraient également déterminer les sanctions ou les peines encourues lorsqu'un signalement n'est pas effectué.

6.35. Les personnes qui sont à la tête des organisations et des installations devraient s'assurer que des mécanismes de signalement officiels ont été mis en place afin d'être informées sur-le-champ de tout incident lié à la sécurité de l'information pour que des mesures correctrices puissent être prises et, s'il y a lieu, pour que l'incident soit signalé aux autorités compétentes. L'embarras ne devrait pas conduire à s'abstenir de signaler un incident lié à la sécurité de l'information, quel que soit le niveau hiérarchique concerné. Les incidents devraient être signalés dans les plus brefs délais afin que des mesures correctrices puissent être prises et qu'il soit possible de dégager des tendances générales.

ENQUÊTES

6.36. Tout incident lié à la sécurité de l'information devrait faire l'objet d'une enquête. Les politiques et les procédures régissant les enquêtes sur ce type d'incident devraient être définies. L'enquête devrait chercher à déterminer si l'incident a eu une faible incidence ou une forte incidence sur la sécurité et la confidentialité de l'information. Les autorités compétentes pourront alors entreprendre toutes les actions appropriées. À titre d'exemple d'incident mineur, on peut citer le fait ne pas avoir enfermé ou protégé correctement un document, sans que cela n'ait entraîné la perte ou la compromission d'informations. Le vol d'un plan de sécurité engendrant une menace stratégique pour une organisation constitue un exemple d'incident majeur.

6.37. Dans le cadre d'une enquête, il conviendrait d'effectuer les actions suivantes :

a) examiner en détail les circonstances de l'incident afin d'en déterminer la portée, l'ampleur et les effets ;
b) évaluer les conséquences de l'incident et l'ampleur de la compromission qui peut avoir eu lieu ;
c) évaluer la nécessité de mettre en place d'autres actions ou de conduire une enquête plus poussée, en faisant éventuellement intervenir d'autres organismes ;
d) recommander des mesures correctrices ou entreprendre une action afin de limiter ou de réduire au maximum les conséquences de l'incident ;
e) établir un compte rendu des résultats de l'enquête comprenant :
    i) la cause probable de l'incident,
    ii) l'évaluation de l'ampleur de la compromission,
    iii) les effets probables de la compromission,
    iv) d'éventuelles recommandations concernant les améliorations à apporter au programme de sécurité afin d'éviter qu'un incident semblable ne se produise,
    v) d'autres actions recommandées, compte tenu de l'incident qui a eu lieu,
    vi) les enseignements que les intervenants concernés doivent en tirer.

6.38. Les autorités compétentes devraient consigner le nombre et le type des incidents signalés qui sont liés à la sécurité de l'information. Les incidents récurrents ou les tendances générales relatives aux défaillances de sécurité devraient être recensés et peuvent donner à penser qu'il y a lieu de faire évoluer la politique de sécurité ou d'améliorer les procédures ou les programmes de

sécurité. Les dernières tendances et les derniers changements devraient faire partie de la formation de sensibilisation afin d'entretenir une culture de sécurité appropriée chez les salariés et dans les entreprises extérieures. Les organisations et les installations devraient aussi tenir à jour leurs propres dossiers.

RÉFÉRENCES

[1] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Objectif et éléments essentiels du régime de sécurité nucléaire d'un État, collection Sécurité nucléaire de l'AIEA n° 20, AIEA, Vienne (2014).

[2] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Recommandations de sécurité nucléaire sur la protection physique des matières nucléaires et des installations nucléaires (INFCIRC/225/Rev.5), collection Sécurité nucléaire de l'AIEA n° 13, AIEA, Vienne (2011).

[3] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Recommandations de sécurité nucléaire relatives aux matières radioactives et aux installations associées, collection Sécurité nucléaire de l'AIEA n° 14, AIEA, Vienne (2011).

[4] OFFICE EUROPÉEN DE POLICE, AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, ORGANISATION DE L'AVIATION CIVILE INTERNATIONALE, ORGANISATION INTERNATIONALE DE POLICE CRIMINELLE-INTERPOL, INSTITUT INTERRÉGIONAL DE RECHERCHE DES NATIONS UNIES SUR LA CRIMINALITÉ ET LA JUSTICE, OFFICE DES NATIONS UNIES CONTRE LA DROGUE ET LE CRIME, ORGANISATION MONDIALE DES DOUANES, Recommandations de sécurité nucléaire sur les matières nucléaires et autres matières radioactives non soumises à un contrôle réglementaire, collection Sécurité nucléaire de l'AIEA n° 15, AIEA, Vienne (2011).

[5] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Mesures de prévention et de protection contre les menaces internes, collection Sécurité nucléaire de l'AIEA n° 8, AIEA, Vienne (2012).

[6] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, La sécurité informatique dans les installations nucléaires, collection Sécurité nucléaire de l'AIEA n° 17, AIEA, Vienne (2013).

[7] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Élaboration, utilisation et actualisation de la menace de référence, collection Sécurité nucléaire de l'AIEA n° 10, AIEA, Vienne (2012).

[8] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Système de gestion des installations et des activités, collection Normes de sûreté de l'AIEA n° GS-R-3, AIEA, Vienne (2011).

[9] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Culture de sécurité nucléaire, collection Sécurité nucléaire de l'AIEA n° 7, AIEA, Vienne (2009).

Annexe I

SYSTÈME DE CLASSIFICATION ET DÉFINITIONS

I–1. L'annexe I donne un exemple de système de classification. Chaque État peut concevoir et utiliser n'importe quel système de classification approprié pour indiquer le niveau de sensibilité d'informations relevant de la sécurité nucléaire. Les définitions qui figurent ci-après correspondent à un système à quatre niveaux similaire à celui que l'on rencontre dans un grand nombre d'États Membres. Le quatrième niveau (TRÈS SECRET) n'est pas abordé, l'expérience ayant montré que, pour des activités nucléaires civiles, il est très peu probable que des actifs informationnels réclament un classement TRÈS SECRET. Il est également à noter que, même si on considère que les informations prennent principalement la forme de documents ou de connaissances, du matériel et d'autres objets physiques peuvent être classés lorsqu'il est possible d'obtenir une information classée à partir de l'observation visuelle de leur aspect interne ou externe, de leur structure, de leur fonctionnement, des tests effectués, des applications prévues ou de leur utilisation.

SECRET

I–2. La compromission d'informations ou de documents classés SECRETS aurait probablement l'un des effets suivants :

a) faire naître des tensions internationales ;
b) porter gravement atteinte aux relations intergouvernementales ;
c) menacer directement la vie ou porter gravement préjudice à l'ordre public, à la sécurité individuelle ou à la liberté individuelle ;
d) porter gravement atteinte à l'efficacité opérationnelle ou à la sécurité des forces nationales de sécurité, ou bien durablement à l'efficacité des opérations de sécurité ou de renseignement très utiles ;
e) occasionner un préjudice matériel substantiel au budget national ou pour des intérêts économiques et commerciaux ;
f) être utile à un individu ou à un groupe préparant un acte malveillant qui pourrait provoquer de très graves dommages dans une installation au moyen de matières nucléaires ou d'autres matières radioactives, ou bien pendant le transport de telles matières.

CONFIDENTIEL

I–3. La compromission d'informations ou de documents classés CONFIDENTIELS aurait probablement l'un des effets suivants :

a) porter atteinte aux relations diplomatiques ;
b) porter préjudice à la sécurité ou à la liberté individuelles ;
c) porter atteinte à l'efficacité opérationnelle ou à la sécurité des forces nationales de sécurité, ou bien à l'efficacité d'opérations de sécurité ou de renseignement utiles ;
d) nuire profondément au budget national ou à des intérêts économiques et commerciaux ;
e) porter substantiellement atteinte à la viabilité financière d'organisations importantes ;
f) entraver une enquête ou faciliter la commission d'infractions graves ;
g) entraver gravement l'élaboration ou la mise en œuvre de politiques publiques importantes ;
h) arrêter ou perturber fortement des opérations nationales importantes ;
i) être utile à un individu ou à un groupe préparant un acte malveillant qui pourrait provoquer de graves dommages dans une installation au moyen de matières nucléaires ou d'autres matières radioactives, ou bien pendant le transport de telles matières.

RESTREINT

I–4. La compromission d'informations ou de documents classés RESTREINTS aurait probablement l'un des effets suivants :

a) peser sur les relations diplomatiques ;
b) provoquer un trouble important chez des personnes ;
c) rendre plus difficile le maintien de l'efficacité opérationnelle ou de la sécurité des forces nationales de sécurité ;
d) entraîner une perte financière ou un manque à gagner pour des personnes ou des entreprises ou contribuer à ce que des personnes ou des entreprises obtiennent un gain ou un avantage indus ;
e) être préjudiciable pour une enquête sur une infraction ;
f) faciliter la commission d'une infraction ;
g) violer des dispositions adéquates visant à maintenir la confidentialité d'informations fournies par des tiers ;

h) entraver l'élaboration ou la mise en œuvre efficaces de politiques publiques ;
i) passer outre les restrictions légales à la divulgation d'informations ;
j) désavantager le gouvernement dans des négociations commerciales ou politiques ;
k) nuire à la bonne gestion du secteur public et à ses activités ;
l) être utile à un individu ou à un groupe préparant un acte malveillant qui pourrait provoquer des dommages importants dans une installation au moyen de matières nucléaires ou d'autres matières radioactives, ou bien pendant le transport de telles matières.

I–5. En ce qui concerne l'application des niveaux de classification présentés ci-dessus au contrôle des informations sensibles, il conviendrait de s'attacher à la manière dont la divulgation non autorisée de ce type d'information pourrait aider un adversaire potentiel pour :

a) choisir une cible pour un vol ou un sabotage de matières nucléaires ou d'autres matières radioactives, sur un équipement ou dans une installation ;
b) préparer ou commettre un vol ou un sabotage de matières nucléaires, d'autres matières radioactives, sur un équipement ou dans une installation :
    i) conception des systèmes de sécurité,
    ii) plans de construction,
    iii) méthodes et procédures appliquées pour le transfert, le contrôle et la manipulation des matières nucléaires et des autres matières radioactives,
    iv) plans, procédures et moyens de sécurité ;
c) évaluer la réussite d'un vol ou d'un sabotage de matières nucléaires, d'autres matières radioactives, sur un équipement ou dans une installation :
    i) conséquences réelles ou hypothétiques du sabotage d'installations ou d'équipements essentiels ;
d) fabriquer illégalement un dispositif nucléaire explosif, un engin à dispersion de radioactivité ou un dispositif d'irradiation :
    i) renseignements descriptifs utiles pour mettre au point un dispositif,
    ii) emplacement des matières nécessaires à la fabrication d'un dispositif,
    iii) emplacement d'une arme nucléaire ;
e) disperser des matières nucléaires ou d'autres matières radioactives dans l'environnement :
    i) emplacement, forme et quantité de matières.

Annexe II

EXEMPLES D'INFORMATIONS SENSIBLES

II–1. L'annexe II présente un exemple de catégorisation relative à la sécurité pour les informations ayant trait à la sécurité nucléaire. Chaque État devrait décider du niveau exact de classification à appliquer à toutes les informations de ce type. Le tableau II-1 donne des exemples d'informations sensibles et indique les points liés à la sensibilité dans chaque cas. Lorsqu'il n'est pas recommandé de communiquer une information, le tableau avance des raisons et indique si la sécurité pourrait être garantie.

II–2. Les catégories d'informations qui sont présentées dans le tableau II-1 ne sont que des exemples de ce que l'on pourrait considérer comme des informations sensibles. Elles ne forment pas une liste exhaustive ou un modèle complet. C'est uniquement à la suite d'une évaluation spécifique menée par l'État concerné que des catégories seront insérées dans un tableau national similaire.

II–3. Dans chaque ligne du tableau, la première colonne donne un exemple type d'information. La deuxième colonne indique si cette catégorie s'applique habituellement aux matières nucléaires et aux installations nucléaires (N), aux autres matières radioactives et aux installations associées (R) ou aux deux (N, R). La troisième colonne précise si les informations présentées pourraient être considérées comme sensibles ou non. Enfin, la dernière colonne donne quelques explications sur la sensibilité des informations et les raisons pour lesquelles elles doivent être protégées.

II–4. S'agissant de l'application du qualificatif sensible à une information et de l'attribution d'un éventuel niveau de classification, il conviendrait de prendre en considération les informations qui ont déjà été publiées et de toute compromission antérieure ou éventuelle compromission des informations. Il peut être irréaliste d'attribuer et de gérer un niveau de classification pour ce type d'information.

II–5. Il conviendrait également d'envisager de qualifier des informations non sensibles de sensibles si, associées à d'autres informations non sensibles, elles peuvent servir à découvrir des informations sensibles.

TABLEAU II–1. CATÉGORISATION THÉORIQUE RELATIVE À LA SÉCURITÉ POUR LES INFORMATIONS AYANT TRAIT À LA SÉCURITÉ NUCLÉAIRE

Catégorie	Domaine	Sensibilité	Raisons de la protection
1. SÉCURITÉ DES MATIÈRES ET DES INSTALLATIONS			
1.1. Réglementation et orientations			
A. Réglementation nationale en matière de sécurité régissant l'utilisation des matières nucléaires et des autres matières radioactives	N, R	Non sensible	Ces informations sont généralement publiées.
B. Orientations concernant cette réglementation, établies par l'autorité compétente ou par un autre organisme public	N, R	Sensible	Même si l'intégralité de ces orientations n'est pas nécessairement sensible, un document de cette nature peut contenir des renseignements sur les normes, les types de matériel à utiliser, les procédures et les opérations de sécurité dans une installation. De tels renseignements pourraient être utiles à des adversaires qui préparent un acte malveillant.
1.2. Politiques nationales de sécurité nucléaire			
A. Politiques publiques générales sur les questions mettant en jeu des matières nucléaires ou d'autres matières radioactives	N, R	Non sensible	Ces informations sont généralement publiques.
B. Politique détaillée portant sur des thèmes de sécurité spécifiques	N, R	Sensible	Elle pourrait donner des indications sur les types d'obstacles que des adversaires auront à affronter, leur permettant de se préparer afin d'obtenir des informations plus détaillées.

TABLEAU II–1. CATÉGORISATION THÉORIQUE RELATIVE À LA SÉCURITÉ POUR LES INFORMATIONS AYANT TRAIT À LA SÉCURITÉ NUCLÉAIRE (suite)

Catégorie	Domaine	Sensibilité	Raisons de la protection
1.3. Plans de sécurité des installations	N, R	Sensible	Ils contiennent généralement des descriptions détaillées des mesures de sécurité en vigueur sur un site et des renseignements précis concernant l'endroit où les matières sont entreposées sur le site concerné. Pour les installations nucléaires, les plans contiennent également des renseignements sur d'autres zones essentielles pour l'exploitation du site.
1.4. Rapports relatifs à la sécurité			
A. Rapports d'enquête, d'inspection et d'évaluation sur la sécurité et autres rapports sur les mesures de protection physique ou de sécurité technique appliquées sur un site ou dans une installation	N, R	Sensible	La consultation de ces rapports peut donner à des adversaires des renseignements sur l'emplacement des matières, les mesures prises pour les protéger et les éventuelles vulnérabilités constatées, les aidant ainsi à contourner les mesures de sécurité et à échapper aux contrôles de même nature.
B. Rapports présentant des caractéristiques essentielles ou mettant en lumière des prescriptions pour améliorer la sécurité, y compris dans des zones essentielles (s'il y a lieu)	N, R	Sensible	Les informations de cette nature peuvent être utiles à des adversaires qui souhaitent contourner les dispositifs de sécurité et pourraient les aider à s'attaquer à une installation.

TABLEAU II–1. CATÉGORISATION THÉORIQUE RELATIVE À LA SÉCURITÉ POUR LES INFORMATIONS AYANT TRAIT À LA SÉCURITÉ NUCLÉAIRE (suite)

Catégorie	Domaine	Sensibilité	Raisons de la protection
C. Résultats d'enquêtes sur la sécurité menées sur un site ou dans une installation, y compris celles qui portent sur les fuites et les pertes d'informations sensibles	N, R	Sensible	Les informations de cette nature peuvent être utiles à des adversaires qui souhaitent contourner les dispositifs de sécurité et pourraient les aider à s'attaquer à une installation.
D. Rapports décrivant les vulnérabilités du système de gestion de la sécurité et les conséquences d'une défaillance	N, R	Sensible	Les informations de cette nature peuvent être utiles à des adversaires qui souhaitent contourner les dispositifs de sécurité.
1.5. Caractéristiques de la construction			
A. Caractéristiques de la construction et de la disposition des lieux où des matières peuvent être entreposées ou traitées, y compris les dessins et les plans conservés sur n'importe quel support, qui montrent des éléments de protection physique servant à prévenir les actes malveillants	N, R	Sensible	Les cartes et plans officiels d'un site peuvent être communiqués si la direction le décide, dans la mesure où ils n'indiquent pas les fonctions d'un bâtiment, les matières qui y sont entreposées, l'emplacement des clôtures de sécurité internes et les autres mesures de sécurité appliquées dans le bâtiment concerné.
B. Caractéristiques de la construction des zones essentielles dans les centrales nucléaires et les autres installations nucléaires	N	Sensible	Les informations de cette nature peuvent aider des adversaires à contourner les dispositifs de sécurité et peuvent éventuellement faciliter le choix d'une cible à des fins de sabotage.

TABLEAU II–1. CATÉGORISATION THÉORIQUE RELATIVE À LA SÉCURITÉ POUR LES INFORMATIONS AYANT TRAIT À LA SÉCURITÉ NUCLÉAIRE (suite)

Catégorie	Domaine	Sensibilité	Raisons de la protection
1.6. Systèmes de protection			
A. Renseignements sur tout dispositif de protection physique : alarmes, caméras de surveillance, contrôle d'accès, personnel de sécurité, etc.	N, R	Sensible	Tout renseignement de cette nature serait utile à un adversaire qui souhaiterait contourner les systèmes de sécurité d'une installation.
B. Types et emplacement des capteurs des systèmes de détection des intrusions, des caméras de surveillance associées et des schémas de câblage, emplacement des alimentations électriques essentielles et des passages de câbles et programmes d'entretien et de test pour ces équipements	N, R	Sensible	
1.7. Renseignements sur les systèmes de contrôle d'accès automatisés, y compris l'emplacement des serveurs informatiques, des serveurs de sauvegarde et de leurs alimentations électriques	N, R	Sensible	Tout renseignement qui pourrait permettre à un adversaire externe ou interne de contourner le système de contrôle d'accès ne devrait pas être communiqué.
1.8. Magasins : procédures de sécurité relatives à la délivrance, à la réception et au contrôle du stock de matières ; nom des détenteurs de clés autorisés ; mesures de surveillance et de gardiennage	N, R	Sensible	Peuvent être utiles à des adversaires qui préparent des actes malveillants.
1.9. Cartes générales montrant la position et les limites d'une installation, mais ne donnant aucun renseignement sur ce qu'elle renferme	N, R	Non sensible	Sur Internet, des applications de cartographie en libre accès permettent d'obtenir clairement de telles informations.

TABLEAU II–1. CATÉGORISATION THÉORIQUE RELATIVE À LA SÉCURITÉ POUR LES INFORMATIONS AYANT TRAIT À LA SÉCURITÉ NUCLÉAIRE (suite)

Catégorie	Domaine	Sensibilité	Raisons de la protection
1.10. Autres questions liées à la protection physique : emplacement, organisation, effectifs et appareils du poste central de sécurité ; emplacement du poste de sécurité secondaire ; type de barrière pour la zone intérieure	N, R	Sensible	Tout renseignement de cette nature serait très utile à un adversaire qui souhaiterait contourner les systèmes de sécurité d'une installation nucléaire.
2. INFORMATIONS RELATIVES À LA QUANTITÉ ET À LA FORME DES MATIÈRES			
2.1. Informations sur la quantité, le type et la forme des matières nucléaires, sources comprises, reçues ou conservées à des endroits précis dans tous les types de sites et de centrales nucléaires, y compris les lieux exacts où du combustible usé est conservé	N	Sensible	Ce type d'information pourrait être utile à des adversaires qui choisissent des cibles lorsqu'ils préparent des attaques.
2.2. Débit : capacité nominale, débit réel et données rétrospectives sur le débit dans une installation soumise au régime des garanties de l'AIEA	N	Non sensible	Ces informations générales sont souvent publiques, en particulier pour les centrales nucléaires.
2.3. Inventaires nationaux ou locaux d'autres matières radioactives (y compris des matières retirées du service) indiquant leur quantité, leur type, leur forme et leur emplacement exact	R	Sensible	Ce type d'information pourrait être utile à des adversaires qui choisissent des cibles lorsqu'ils préparent des attaques pour voler des matières radioactives. Pour ces inventaires, il conviendrait de déterminer quelles informations sont déjà accessibles au public. Ces informations ne sont pas toutes considérées comme sensibles. Les méthodes qui s'appuient sur la connaissance du risque aident à déterminer si une information doit être qualifiée de sensible.

TABLEAU II–1. CATÉGORISATION THÉORIQUE RELATIVE À LA SÉCURITÉ POUR LES INFORMATIONS AYANT TRAIT À LA SÉCURITÉ NUCLÉAIRE (suite)

Catégorie	Domaine	Sensibilité	Raisons de la protection
3. TRANSPORT DE MATIÈRES (Y COMPRIS LES DÉPLACEMENTS À L'INTÉRIEUR D'UN SITE)			
3.1. Informations sur les mouvements de matières nucléaires de catégorie I, II ou III	N	Sensible	Ce type d'information pourrait aider à choisir des cibles dans le cadre de la préparation d'actes malveillants mettant en jeu des matières nucléaires pendant leur transport.
3.2. Véhicules hautement protégés (VHP)			
A. Accès visuel à l'intérieur de la cabine du conducteur et du compartiment de chargement	N	Sensible	Les VHP sont des véhicules spécialement conçus pour transporter des matières nucléaires en toute sécurité. Ainsi, toutes les informations dont le type est énuméré dans la présente section pourraient être utiles à un adversaire préparant une tentative de vol ou de sabotage de matières nucléaires pendant leur transport.
B. Caractéristiques de la conception et de la construction du véhicule relatives à la sécurité physique	N	Sensible	
C. Conception et rôle des alarmes, des systèmes d'immobilisation et des clés destinées à des serrures spéciales	N	Sensible	
D. Clés du compartiment de chargement, clés de secours et code de la serrure à combinaison, si une telle serrure est utilisée	N	Sensible	
E. Système de géolocalisation du véhicule, si un tel système est installé sur le VHP ; fonctionnement du système et communications	N	Sensible	

TABLEAU II–1. CATÉGORISATION THÉORIQUE RELATIVE À LA SÉCURITÉ POUR LES INFORMATIONS AYANT TRAIT À LA SÉCURITÉ NUCLÉAIRE (suite)

Catégorie	Domaine	Sensibilité	Raisons de la protection
3.3. Conteneurs de transport de matières nucléaires			
A. Degré de résistance des conteneurs de transport aux attaques menées par différents moyens	N	Sensible	Utile pour un adversaire qui prépare un sabotage dans le but de disséminer des matières nucléaires ou qui projette de voler des matières pendant un transport.
B. Caractéristiques des conteneurs et données techniques les concernant	N	Non sensible	Sur Internet, on trouve souvent des informations sur la conception de ces conteneurs, sans renseignements détaillés sur la construction de ce type de matériel.
C. Informations sur la conception de conteneurs particuliers (conteneurs spécialement protégés)	N	Sensible	Utile pour un adversaire qui prépare un sabotage dans le but de disséminer des matières nucléaires ou qui projette de voler des matières pendant un transport.
3.4. Colis de transport : informations sur la conception des colis de transport	N	Sensible	Utile pour un adversaire qui prépare un sabotage dans le but de disséminer des matières nucléaires ou qui projette de voler des matières pendant un transport.
3.5. Informations sur les mouvements d'autres matières radioactives	R	Sensible	Ce type d'information, en particulier s'il concerne le transport de sources de rayonnements puissantes, pourrait être utilisé pour préparer un vol de matières.

TABLEAU II–1. CATÉGORISATION THÉORIQUE RELATIVE À LA SÉCURITÉ POUR LES INFORMATIONS AYANT TRAIT À LA SÉCURITÉ NUCLÉAIRE (suite)

Catégorie	Domaine	Sensibilité	Raisons de la protection
4. SYSTÈMES INFORMATIQUES IMPORTANTS POUR LA SÉCURITÉ ET LA SÛRETÉ			
4.1. Renseignements sur les systèmes informatiques où sont stockées et traitées des informations sensibles, y compris les systèmes utilisés à des fins de sécurité, l'architecture système, les mesures de sécurité informatique appliquées et l'emplacement des supports de sauvegarde	N, R	Sensible	Informations utiles pour un adversaire qui se prépare à commettre un acte malveillant dans une installation.
4.2. Renseignements sur les systèmes de contrôle d'accès, les systèmes de détection des intrusions, les systèmes d'alarme, les systèmes d'évaluation et de surveillance et sur d'autres fonctions et dispositifs de sécurité ; emplacement du matériel et des logiciels de sauvegarde	N, R	Sensible	Informations utiles pour un adversaire qui se prépare à commettre un acte malveillant dans une installation.
4.3. Renseignements sur les systèmes informatiques liés à la sûreté, notamment leur emplacement, leur rôle, les chemins de mise à jour, les alimentations électriques et les sauvegardes	N, R	Sensible	Ces systèmes sont dotés de fonctions de contrôle et de suivi des opérations. Si un adversaire parvenait à les compromettre, il pourrait, au minimum, perturber l'exploitation d'une installation et, dans le pire des cas, les perturbations pourraient provoquer un rejet de matières radioactives.

TABLEAU II–1. CATÉGORISATION THÉORIQUE RELATIVE À LA SÉCURITÉ POUR LES INFORMATIONS AYANT TRAIT À LA SÉCURITÉ NUCLÉAIRE (suite)

Catégorie	Domaine	Sensibilité	Raisons de la protection
5. AGENTS DE SÉCURITÉ ET FORCES D'INTERVENTION			
5.1. Agents de sécurité dans une installation			
A. Effectif global et moyens actuels	N	Non sensible	Rendre public l'existence d'agents de sécurité peut rassurer le public et avoir un effet dissuasif.
B. Effectif et moyens actuels sur un site particulier	N	Sensible	Les informations de cette nature peuvent être utiles à un adversaire qui prépare une intrusion dans un site nucléaire à des fins de sabotage ou de vol et pourraient miner la capacité à réagir efficacement en cas d'attaque.
C. Taille des équipes sur un site	N	Sensible	
D. Armes et autre matériel spécial mis à la disposition des agents de sécurité et nombre d'utilisateurs entraînés à la manipulation des armes à feu parmi les agents de sécurité d'un site particulier	N	Sensible	Toutes les informations qui pourraient aider un adversaire à estimer à l'avance l'ampleur de la réaction et les moyens dont dispose une entité opérationnelle tactique devraient être protégées contre la divulgation.
E. Emplacement, moyens, armes et véhicules spéciaux d'intervention de la force d'intervention et délai d'intervention sur un site	N	Sensible	
F. Plans d'intervention	N	Sensible	

TABLEAU II–1. CATÉGORISATION THÉORIQUE RELATIVE À LA SÉCURITÉ POUR LES INFORMATIONS AYANT TRAIT À LA SÉCURITÉ NUCLÉAIRE (suite)

Catégorie	Domaine	Sensibilité	Raisons de la protection
5.2. Escortes accompagnant le transport de matières nucléaires			
A. Déploiement et moyens de l'escorte	N	Sensible	Ces informations pourraient être utiles à un adversaire qui prévoit d'attaquer un convoi.
B. Radiofréquences utilisées pour communiquer avec une force d'intervention ou la police locale	N	Sensible	
6. COMPTABILITÉ DES MATIÈRES NUCLÉAIRES			
6.1. Description			
A. Principes généraux de la comptabilité des matières nucléaires	N	Non sensible	Des principes généraux de ce type ont été publiés.
B. Questionnaire concernant les renseignements descriptifs, réponse à ce questionnaire et emplacement des zones de bilan matières (ZBM) et des points de mesure principaux (PMP)	N	Sensible	De telles informations détaillées sur l'emplacement et les quantités de matières nucléaires pourraient être utiles à un adversaire qui prépare un acte malveillant.
C. Forme physique et chimique des matières qui font l'objet de mesures aux PMP	N	Sensible	
6.2. Mesures et résultats des instruments de mesure			
A. Précision et exactitude des techniques courantes de laboratoire	N	Non sensible	Ces informations sont souvent publiques.

TABLEAU II–1. CATÉGORISATION THÉORIQUE RELATIVE À LA SÉCURITÉ POUR LES INFORMATIONS AYANT TRAIT À LA SÉCURITÉ NUCLÉAIRE (suite)

Catégorie	Domaine	Sensibilité	Raisons de la protection
B. Chiffres montrant la sensibilité des mesures ou les seuils d'alarme pour la différence d'inventaire (DI) dans une centrale particulière	N	Sensible	Les chiffres relatifs à la précision et à l'exactitude des mesures réelles ou caractéristiques, qu'ils soient agrégés ou détaillés, pourraient être utiles à un adversaire qui prépare un vol de matières.
6.3. Données relatives aux flux de matières nucléaires et à l'inventaire de telles matières conservées dans les systèmes informatiques, sur supports papier et sur n'importe quel support de stockage	N	Sensible	Ces informations pourraient révéler un emplacement et des mouvements de matières nucléaires.
6.4. Différence d'inventaire			
A. Chiffres annuels de DI pour un site qui ne révèlent pas la ZBM concernée	N	Non sensible	Dans de nombreux États, les chiffres annuels agrégés de DI sont ou peuvent être publiés.
B. DI dans une ZBM ou à un PMP	N	Sensible	
C. Détails d'une enquête sur un DI particulier, sauf si la communication de ces informations a officiellement été autorisée	N	Sensible	Cependant, des DI détaillées ou des résultats d'enquête pourraient être utiles à un adversaire pour s'attaquer à une installation particulière et devraient donc être considérés comme sensibles.
D. Erreur admissible pour une DI ou autres indications précises quant à l'incertitude qui s'attache aux DI	N	Sensible[a]	

[a] Dans certains États, l'erreur admissible pour une DI n'est pas considérée comme une information sensible.

TABLEAU II–1. CATÉGORISATION THÉORIQUE RELATIVE À LA SÉCURITÉ POUR LES INFORMATIONS AYANT TRAIT À LA SÉCURITÉ NUCLÉAIRE (suite)

Catégorie	Domaine	Sensibilité	Raisons de la protection
7. DEMANDES D'AUTORISATION			
7.1. Demandes d'autorisation qui ne contiennent pas d'informations détaillées sur les mesures de sécurité ni sur le type, la forme et la quantité de matières	N, R	Non sensible	Le contenu d'une telle demande varie en fonction du cadre législatif et réglementaire et de l'utilisation finale prévue. Si la demande contient des informations sensibles qui pourraient être utiles à un adversaire, elle devrait également être traitée comme une information sensible.
7.2. Demandes d'autorisation contenant des informations détaillées, par exemple sur des mesures de sécurité et sur le type, la forme et la quantité de matières	N, R	Sensible	Le contenu d'une telle demande varie en fonction du cadre législatif et réglementaire et de l'utilisation finale prévue. Si la demande contient des informations sensibles qui pourraient être utiles à un adversaire, elle devrait également être traitée comme une information sensible.
8. ARGUMENTAIRES DE SÛRETÉ, DOCUMENTS TECHNIQUES ET AUTRES INFORMATIONS RELATIVES À LA SÛRETÉ OU À L'ENVIRONNEMENT			
8.1. Argumentaires de sûreté de toutes catégories			La plupart des informations qui figurent dans les argumentaires de sûreté peuvent être rendues publiques pour des questions de transparence, mais certaines d'entre elles peuvent être considérées comme sensibles au regard de la sécurité nucléaire.

TABLEAU II–1. CATÉGORISATION THÉORIQUE RELATIVE À LA SÉCURITÉ POUR LES INFORMATIONS AYANT TRAIT À LA SÉCURITÉ NUCLÉAIRE (suite)

Catégorie	Domaine	Sensibilité	Raisons de la protection
A. Éléments détaillés sur les risques ou autres informations qui pourraient être utilisées pour évaluer les conséquences d'un rejet, ou bien renseignements sur les conséquences des rejets	N, R	Sensible	Ces informations détaillées qui figurent dans les argumentaires de sûreté pourraient être utiles à un adversaire pour choisir des cibles et préparer une opération.
B. Renseignements sur les forces et les faiblesses des procédures, des structures et des systèmes de protection conçus pour contenir, contrôler ou protéger des matières nucléaires ou d'autres matières radioactives	N, R	Sensible	
C. Renseignements sur l'accès au processus de production, qu'il s'agisse du contrôle d'accès physique ou du retrait de matières du processus à des fins de contrôle et de surveillance	N, R	Sensible	
9. PLANS D'URGENCE ET D'INTERVENTION ET EXERCICES			
9.1. Urgence et intervention			
A. Existence d'un plan d'urgence et d'intervention	N, R	Non sensible	Rendre public l'existence d'un plan de ce type peut rassurer la population et avoir un effet dissuasif.
B. Contenu détaillé d'un plan d'urgence et d'intervention	N, R	Sensible	Les détails du plan pourraient indiquer les moyens, les limites et les délais d'intervention, et pourraient donc être utiles à un adversaire qui prépare une attaque.

TABLEAU II–1. CATÉGORISATION THÉORIQUE RELATIVE À LA SÉCURITÉ POUR LES INFORMATIONS AYANT TRAIT À LA SÉCURITÉ NUCLÉAIRE (suite)

Catégorie	Domaine	Sensibilité	Raisons de la protection
9.2. Plans de sécurité d'urgence contenant des informations détaillées	N, R	Sensible	Ces documents contiennent des informations sur les mesures de sécurité en vigueur, sur les moyens de la police ou des agents de sécurité et sur le type d'intervention probable en cas d'incident lié à la sécurité.
9.3. Exercices			
A. Fait qu'un exercice aura ou a eu lieu	N, R	Non sensible	Rendre public l'existence d'exercices peut rassurer la population. Toutefois, il ne faut pas que le niveau de détail fourni, par exemple la date, l'heure ou le lieu d'un futur exercice, puisse être utile à un adversaire.
B. Renseignements sur les exercices de sécurité réalisés sur un site, notamment le scénario, les aspects du plan de sécurité qui font l'objet d'une vérification, la participation éventuelle d'une force d'intervention et les résultats de l'exercice	N, R	Sensible	Donne des informations aux adversaires sur la nature, la taille, les moyens et le délai de réaction de la force d'intervention et des renseignements sur la force d'intervention armée, la nature des tactiques employées et le plan de signalisation.
C. Renseignements sur les exercices de sûreté	N, R	Non sensible	Les exercices de sûreté sont souvent réalisés de manière ouverte et transparente. On peut généralement les considérer comme non sensibles tant qu'ils ne révèlent pas d'informations détaillées sur des mesures de sécurité.

TABLEAU II–1. CATÉGORISATION THÉORIQUE RELATIVE À LA SÉCURITÉ POUR LES INFORMATIONS AYANT TRAIT À LA SÉCURITÉ NUCLÉAIRE (suite)

Catégorie	Domaine	Sensibilité	Raisons de la protection
10. INFORMATIONS PERSONNELLES			
10.1. Informations personnelles			
A. Informations issues des contrôles de fiabilité	N, R	Sensible	Des informations de cette nature pourraient être utilisées pour exercer un chantage ou commettre une extorsion. Dans la plupart des pays, la réglementation relative à la protection de la vie privée impose de protéger ce type d'information.
B. Informations contenues dans les dossiers individuels	N, R	Sensible	
11. INVENTAIRE DES DÉCHETS RADIOACTIFS			
11.1. Informations sur les déchets radioactifs			
A. Informations générales sur les inventaires à l'exclusion des informations qui pourraient être exploitées, par exemple le fait que des déchets soient entreposés dans un site particulier ou la quantité totale de déchets sans préciser leur emplacement	N	Non sensible	Ce type d'information est généralement public et ne donne pas de précisions utiles pour un adversaire.
B. Informations qui pourraient être utilisées pour commettre un acte malveillant ou qui permettent de repérer un bâtiment particulier dans une installation, ainsi que les matières qu'il contient	N	Sensible	Ces informations donnent des renseignements sur les cibles à un adversaire qui prépare un sabotage.

TABLEAU II–1. CATÉGORISATION THÉORIQUE RELATIVE À LA SÉCURITÉ POUR LES INFORMATIONS AYANT TRAIT À LA SÉCURITÉ NUCLÉAIRE (suite)

Catégorie	Domaine	Sensibilité	Raisons de la protection
12. DÉCLASSEMENT			
12.1. Plans de déclassement de centrale	N, R	Non sensible	Les plans de déclassement d'installations sont souvent rendus publics.
12.2. Déchets de déclassement[b]			
A. Fait qu'une installation d'entreposage doive être construite et emplacement de cette installation	N, R	Non sensible	Ces informations sont souvent publiques.
B. Renseignements sur la construction, les mesures de sécurité et le type de matière qui seront entreposées concernant de nouveaux bâtiments destinés au traitement et à l'entreposage des déchets et des matières contaminées résultant d'activités de traitement effectuées pendant un déclassement	N, R	Sensible	Ces informations peuvent donner des renseignements utiles sur les cibles à un adversaire qui prépare un sabotage.
13. ÉVALUATIONS DE LA MENACE ET CRITÈRES APPLIQUÉS POUR DÉCLENCHER DES ALERTES SUR LA SÉCURITÉ			
13.1. Évaluations de la menace établies par l'État, les autorités nationales de sécurité ou d'autres autorités compétentes	N, R	Sensible	Généralement réalisées à partir d'éléments relevant de la sécurité nationale, par exemple des informations obtenues par les services de renseignement.

[b] Il s'agit principalement des matières contaminées extraites d'une installation, plutôt que des déchets radioactifs résultant des processus mis en œuvre pendant son fonctionnement normal..

TABLEAU II–1. CATÉGORISATION THÉORIQUE RELATIVE À LA SÉCURITÉ POUR LES INFORMATIONS AYANT TRAIT À LA SÉCURITÉ NUCLÉAIRE (suite)

Catégorie	Domaine	Sensibilité	Raisons de la protection
13.2. Renseignements sur la menace de référence	N	Sensible	Proviennent généralement d'éléments relevant de la sécurité nationale, par exemple des informations obtenues par les services de renseignement.
13.3. Détails de l'étude visant à recenser les zones essentielles	N	Sensible	Pourraient être utiles à un adversaire pour déterminer les cibles et réaliser une attaque.
13.4. Raisons pour lesquelles un niveau d'alerte de sécurité est adopté ou modifié	N, R	Sensible	Généralement établies à partir d'éléments relevant de la sécurité nationale, par exemple des informations obtenues par les services de renseignement.
14. TECHNIQUES NUCLÉAIRES			
14.1. Informations techniques détaillées sur la production ou le traitement de matières nucléaires (par exemple, le traitement et le retraitement de l'uranium enrichi)	N	Sensible	Les informations de ce type pourraient être utiles à un adversaire.
14.2. Modèles ou nouvelle technique présentés à des fins d'autorisation (réacteur avancé, etc.)	N	Sensible	Même si certains détails sur ces techniques peuvent être rendus publics, certaines particularités du modèle ou de la technique concernés pourraient être utiles à des adversaires à des fins de préparation. Ces informations peuvent être examinées afin d'y rechercher des informations sensibles.

TABLEAU II–1. CATÉGORISATION THÉORIQUE RELATIVE À LA SÉCURITÉ POUR LES INFORMATIONS AYANT TRAIT À LA SÉCURITÉ NUCLÉAIRE (suite)

Catégorie	Domaine	Sensibilité	Raisons de la protection
14.3. Informations détaillées qui faciliteraient le démontage de dispositif afin d'accéder à des sources ou qui contribueraient à contourner d'autres mesures de sécurité	R	Sensible	Ces informations pourraient être utiles à un adversaire qui tente d'enlever des matières radioactives.
14.4. Études de vulnérabilité portant sur des caractéristiques techniques	N, R	Sensible	Si des études menées par des chercheurs peuvent être rendues publiques, toute information détaillée qui présente des vulnérabilités et qui pourrait être exploitée par un adversaire devrait être protégée contre toute divulgation non autorisée.
15. DONNÉES HISTORIQUES			
15.1. Données historiques qui restent pertinentes et sensibles, que ces informations soient classées ou non	N, R	Sensible	En dépit de leur ancienneté, les informations de cette nature peuvent encore être utiles à des adversaires.

Note : DI – différence d'inventaire ; N – matières nucléaires et installations nucléaires ; PMP – point de mesure principal ; R – autres matières radioactives et installations associées ; VHP – véhicule hautement protégé ; ZMB – zone de bilan matières.

Annexe III

EXEMPLE DE PROGRAMME DE SENSIBILISATION À LA SÉCURITÉ

III–1. L'annexe III présente un exemple de cadre et de contenu pour un programme de sensibilisation à la sécurité. Au moment où il doit fixer le contenu d'un programme de sensibilisation à la sécurité, le responsable de la sécurité d'une organisation devrait tenir compte de la pertinence des thèmes et des méthodes exposés ci-après pour ses besoins et adapter le programme en conséquence.

FORMATION À LA SÉCURITÉ

III–2. Les formations se répartissent globalement en quatre catégories :

a) les formations de sensibilisation, qui permettent de mieux connaître les menaces et les vulnérabilités et de comprendre qu'il convient de protéger les données, les informations et les moyens de les traiter (sensibilisation à la sécurité informatique et à la sécurité de l'information) ;
b) les formations thématiques, qui portent sur des aspects particuliers de la sécurité et sont destinées à l'ensemble du personnel (gestion des documents classés et procédures applicables en cas d'incident lié à la sécurité de l'information) ;
c) la formation professionnelle, qui est en général une formation technique détaillée destinée aux membres du personnel ayant des responsabilités particulières, comme les administrateurs système, les développeurs, les administrateurs réseau, les agents de sécurité et les personnes qui déterminent le niveau de classification d'un document ;
d) la formation spécialisée à la sécurité, très spécifique et de haut niveau, habituellement destinée à la direction et qui porte notamment sur la gestion des risques, la prévention des incidents et les interventions en cas d'incident.

III–3. Le programme peut prévoir une sensibilisation sur les sujets suivants :

a) vue d'ensemble du dispositif national de sécurité ;
b) les différents aspects de la sécurité de l'information et les raisons pour lesquelles ils sont importants pour la sécurité nucléaire ;

c) le système national de classification ;
d) les principes fondamentaux de la sécurité, comme le « besoin d'en connaître » et le « besoin de détenir » ;
e) les menaces qui pèsent actuellement sur la sécurité en raison d'actes délibérés commis par :
   i) es services de renseignement ennemis à des fins d'espionnage et de transfert de technologie,
   ii) des organisations subversives,
   iii) d'autres individus ou groupes, comme les courtiers en information et les journalistes d'investigation qui cherchent à accéder sans autorisation à des informations sensibles ou à des sites et à des installations nucléaires,
   iv) des adversaires internes ;
f) les menaces que font peser des organisations rivales et les menaces de sabotage, en tenant compte de la menace mondiale émanant de n'importe quelle faction extrémiste ;
g) les risques et les conséquences d'une perte ou de fuites d'informations sensibles en interne, parfois par inadvertance ou dans l'intention de nuire, ainsi que par trahison pour des motifs politiques ou pour favoriser le terrorisme ;
h) les comportements ou activités susceptibles d'aider des adversaires potentiels ou d'accroître le risque de compromission, notamment :
   i) les comportements risqués, par exemple une attitude désinvolte à l'égard de la sécurité ou des propos imprudents,
   ii) les comportements inconscients qui peuvent attirer l'attention d'organisations ennemies et les précautions à adopter dans les activités quotidiennes, notamment dans le cadre des rencontres, des voyages, de la correspondance et des relations sociales ;
i) les informations sur les événements d'actualité liés à la sécurité et sur les nouvelles méthodes employées par les organisations ennemies qui devraient être diffusées rapidement ;
j) la nécessité de signaler immédiatement toutes les situations suspectes, les faiblesses apparentes des procédures de sécurité ou tout comportement manifestement risqué chez des collègues ; les moyens d'effectuer ces signalements de manière confidentielle devraient être largement exposés ;
k) les effets de lois et règlements nationaux et leur incidence sur les individus, par exemple les lois régissant le secret, la lutte contre le terrorisme, la sécurité, la protection des données et la liberté d'information, ainsi que les sanctions et les peines encourues en cas de violation de la loi ;
l) des explications sur les niveaux d'habilitation de sécurité, sur la manière dont les contrôles de fiabilité sont effectués, sur leur raison d'être dans les

activités nucléaires et radiologiques et sur les correspondances entre les niveaux d'accès et les niveaux d'habilitation et de fiabilité ; explications, en outre, sur la manière dont ces éléments se rattachent aux menaces pour la sécurité susmentionnées ;

m) les dénis de service (par exemple, empêcher une organisation d'accéder à une information quand elle en a besoin, y compris par le vol d'informations) ou la destruction d'informations, des atteintes à la disponibilité ;

n) la modification d'informations ou l'intervention sur des informations non autorisées, une atteinte à l'intégrité ;

o) la divulgation non autorisée, une violation de la confidentialité.

III–4. Le programme pourrait prévoir de former les participants sur les sujets suivants :

a) la sécurité des informations relatives aux matières nucléaires, aux autres matières radioactives et aux installations ;

b) les bonnes pratiques et procédures de sécurité, notamment :
   i) l'utilisation correcte des marques de classification,
   ii) la protection physique, les habilitations de sécurité et la sécurité de l'information (par exemple en ce qui concerne les documents, les communications et les ordinateurs),
   iii) des exemples pratiques de mise en application des règles et des procédures de sécurité aux tâches auxquelles les salariés se livrent ou se livreront,
   iv) les mesures à prendre si l'on soupçonne ou découvre une atteinte à la sécurité.

MÉTHODES COMPLÉMENTAIRES DESTINÉES À FAVORISER LA SÉCURITÉ

III–5. En plus du programme de formation de base, il existe plusieurs autres méthodes qui permettent de sensibiliser les salariés et les entreprises extérieures à la sécurité :

a) publication régulière de bulletins d'information par les autorités nationales de sécurité ; ces bulletins peuvent aborder des questions d'actualité et délivrer des conseils sur divers sujets ayant trait à la sécurité ;

b) affiches rappelant aux personnes les menaces qui pèsent sur la sécurité et les principales mesures de sécurité nécessaires pour les contrer ; comme leur effet est généralement temporaire, elles doivent être placées bien en évidence, mais aussi changées fréquemment ;

c) autocollants rappelant aux salariés leur responsabilité personnelle en matière de maintien de la sécurité lorsqu'ils utilisent du matériel spécifique ;
d) affichage de rappels sur la sécurité au démarrage d'un système informatique, que l'utilisateur doit confirmer avoir lu avant que l'ordinateur n'achève la phase de démarrage ou d'ouverture de session (les systèmes peuvent enregistrer de telles confirmations, de sorte qu'un utilisateur ne pourra pas affirmer qu'il n'a pas vu le rappel) ;
e) notes, bulletins et circulaires de sécurité rédigés par la direction de la sécurité, notamment pour rappeler au personnel certaines règles en la matière et pour éviter qu'il ne fasse preuve d'une confiance excessive ;
f) faire connaître des cas d'atteintes à la sécurité et les enseignements qui peuvent en être tirés ;
g) prévenir les personnes de menaces particulières ou actuelles pour la sécurité et donner des orientations pour les contrer ;
h) mettre en place des moyens de communication avec les individus sur les questions de sécurité en général ;
i) contrôler régulièrement les connaissances des personnes dans le domaine de la sécurité ;
j) l'intranet d'une organisation peut aussi être un outil précieux pour évoquer et promouvoir la sécurité, à condition que le niveau de classification des documents présentés, au vu de leur nature et de leur sensibilité, ne soit pas supérieur à ce que peut accepter le réseau.

GLOSSAIRE

autorité compétente. Organisation ou institution publique qui a été désignée par un État pour assurer une ou plusieurs fonctions ayant trait à la sécurité nucléaire.

autre matière radioactive. Toute matière radioactive qui n'est pas une matière nucléaire.

besoin de détenir. Règle selon laquelle les personnes ne sont autorisées à avoir en leur possession que les actifs informationnels qui leur sont nécessaires pour pouvoir travailler efficacement.

besoin d'en connaître. Règle selon laquelle les personnes, les processus et les systèmes n'ont accès qu'aux informations, moyens et actifs qui sont nécessaires à l'exécution des fonctions autorisées.

compromission. Violation de la confidentialité, perte d'intégrité ou perte de disponibilité, de nature accidentelle ou délibérée, d'un objet informationnel.

confidentialité. Propriété selon laquelle une information n'est pas rendue accessible ou divulguée à des personnes, entités ou processus non autorisés.

disponibilité. Propriété d'être accessible et utilisable à la demande par une entité autorisée.

information sensible. Information, quelle qu'en soit la forme, logiciel inclus, dont la divulgation, la modification, la transformation, la destruction ou le refus d'utilisation non autorisés pourraient compromettre la sécurité nucléaire.

intégrité. Exactitude et exhaustivité de l'information.

matière nucléaire. Tout produit fissile spécial ou toute matière brute tels qu'ils sont définis à l'article XX du Statut de l'AIEA.

matière radioactive. Toute matière désignée en droit interne ou par un organisme de réglementation comme devant faire l'objet d'un contrôle réglementaire en raison de sa radioactivité.

objet informationnel. Connaissances ou données ayant de la valeur pour l'organisation.

ressources d'informations sensibles. Tous appareils ou éléments utilisés pour stocker, traiter, contrôler ou transmettre des informations sensibles. Les ressources d'informations sensibles comprennent notamment les dispositifs de contrôle, les réseaux, les systèmes d'information et tous les autres supports électroniques ou physiques.

sécurité de l'information. Protection de la confidentialité, de l'intégrité et de la disponibilité de l'information.

IAEA
Agence internationale de l'énergie atomique

N° 25

OÙ COMMANDER ?

Dans les pays suivants, vous pouvez vous procurer les publications de l'AIEA disponibles à la vente chez nos dépositaires ci-dessous ou dans les grandes librairies.

Les publications non destinées à la vente doivent être commandées directement à l'AIEA. Les coordonnées figurent à la fin de la liste ci-dessous.

ALLEMAGNE

Goethe Buchhandlung Teubig GmbH
Schweitzer Fachinformationen
Willstätterstrasse 15, 40549 Düsseldorf, ALLEMAGNE
Téléphone : +49 (0) 211 49 874 015 • Fax : +49 (0) 211 49 874 28
Courriel : kundenbetreuung.goethe@schweitzer-online.de • Site web : www.goethebuch.de

CANADA

Renouf Publishing Co. Ltd
22-1010 Polytek Street, Ottawa, ON K1J 9J1, CANADA
Téléphone : (+1 613) 745 2665 • Fax : +1 643 745 7660
Courriel : order@renoufbooks.com • Site web : www.renoufbooks.com

Bernan / Rowman & Littlefield
15200 NBN Way, Blue Ridge Summit, PA 17214, ÉTATS-UNIS D'AMÉRIQUE
Téléphone : +1 800 462 6420 • Fax : +1 800 338 4550
Courriel : orders@rowman.com • Site web : www.rowman.com/bernan

ÉTATS-UNIS D'AMÉRIQUE

Bernan / Rowman & Littlefield
15200 NBN Way, Blue Ridge Summit, PA 17214, ÉTATS-UNIS D'AMÉRIQUE
Téléphone : +1 800 462 6420 • Fax : +1 800 338 4550
Courriel : orders@rowman.com• Site web : www.rowman.com/bernan

Renouf Publishing Co. Ltd
812 Proctor Avenue, Ogdensburg, NY 13669-2205, ÉTATS-UNIS D'AMÉRIQUE
Téléphone : +1 888 551 7470 • Fax : +1 888 551 7471
Courriel : orders@renoufbooks.com • Site web : www.renoufbooks.com

FÉDÉRATION DE RUSSIE

Scientific and Engineering Centre for Nuclear and Radiation Safety
107140, Moscou, Malaya Krasnoselskaya st. 2/8, bld. 5, FÉDÉRATION DE RUSSIE
Téléphone : +7 499 264 00 03 • Fax : +7 499 264 28 59
Courriel : secnrs@secnrs.ru • Site web : www.secnrs.ru

FRANCE

Form-Edit
5 rue Janssen, B.P. 25, 75921 Paris CEDEX, FRANCE
Téléphone : +33 1 42 01 49 49 • Fax : +33 1 42 01 90 90
Courriel : formedit@formedit.fr • Site web : www.form-edit.com

INDE

Allied Publishers

1st Floor, Dubash House, 15, J.N. Heredi Marg, Ballard Estate, Mumbai 400001, INDE
Téléphone : +91 22 4212 6930/31/69 • Fax : +91 22 2261 7928
Courriel : alliedpl@vsnl.com • Site web : www.alliedpublishers.com

Bookwell

3/79 Nirankari, Delhi 110009, INDE
Téléphone : +91 11 2760 1283/4536
Courriel : bkwell@nde.vsnl.net.in • Site web : www.bookwellindia.com

ITALIE

Libreria Scientifica "AEIOU"

Via Vincenzo Maria Coronelli 6, 20146 Milan, ITALIE
Téléphone : +39 02 48 95 45 52 • Fax : +39 02 48 95 45 48
Courriel : info@libreriaaeiou.eu • Site web : www.libreriaaeiou.eu

JAPON

Maruzen-Yushodo Co., Ltd

10-10 Yotsuyasakamachi, Shinjuku-ku, Tokyo 160-0002, JAPON
Téléphone : +81 3 4335 9312 • Fax : +81 3 4335 9364
Courriel : bookimport@maruzen.co.jp • Site web : www.maruzen.co.jp

RÉPUBLIQUE TCHÈQUE

Suweco CZ, s.r.o.

Sestupná 153/11, 162 00 Prague 6, RÉPUBLIQUE TCHÈQUE
Téléphone : +420 242 459 205 • Fax : +420 284 821 646
Courriel : nakup@suweco.cz • Site web : www.suweco.cz

Les commandes de publications destinées ou non à la vente peuvent être adressées directement à :

Unité de la promotion et de la vente
Agence internationale de l'énergie atomique
Centre international de Vienne, B.P. 100, 1400 Vienne, AUTRICHE
Téléphone : +43 1 2600 22529 ou 22530 • Fax : +43 1 2600 29302 ou +43 1 26007 22529
Courriel : sales.publications@iaea.org • Site web : www.iaea.org/books

16-38622

La sécurité des informations sensibles relatives à la sécurité nucléaire constitue un principe fondamental. Une information sensible est une information dont la divulgation (ou la modification, la transformation, la destruction ou le refus d'utilisation) non autorisée pourrait compromettre la sécurité nucléaire ou faciliter la commission d'un acte malveillant contre une installation, une organisation ou un transport nucléaires. Le présent guide d'application définit les concepts de base de la sécurité de l'information tels qu'ils pourraient s'appliquer à la sécurité nucléaire afin d'aider les États Membres et les organisations qui ont des responsabilités en matière de sécurité nucléaire à élaborer un régime de sécurité de l'information.

AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE
VIENNE
ISBN 978–92–0–204317–6
ISSN 2520–6931