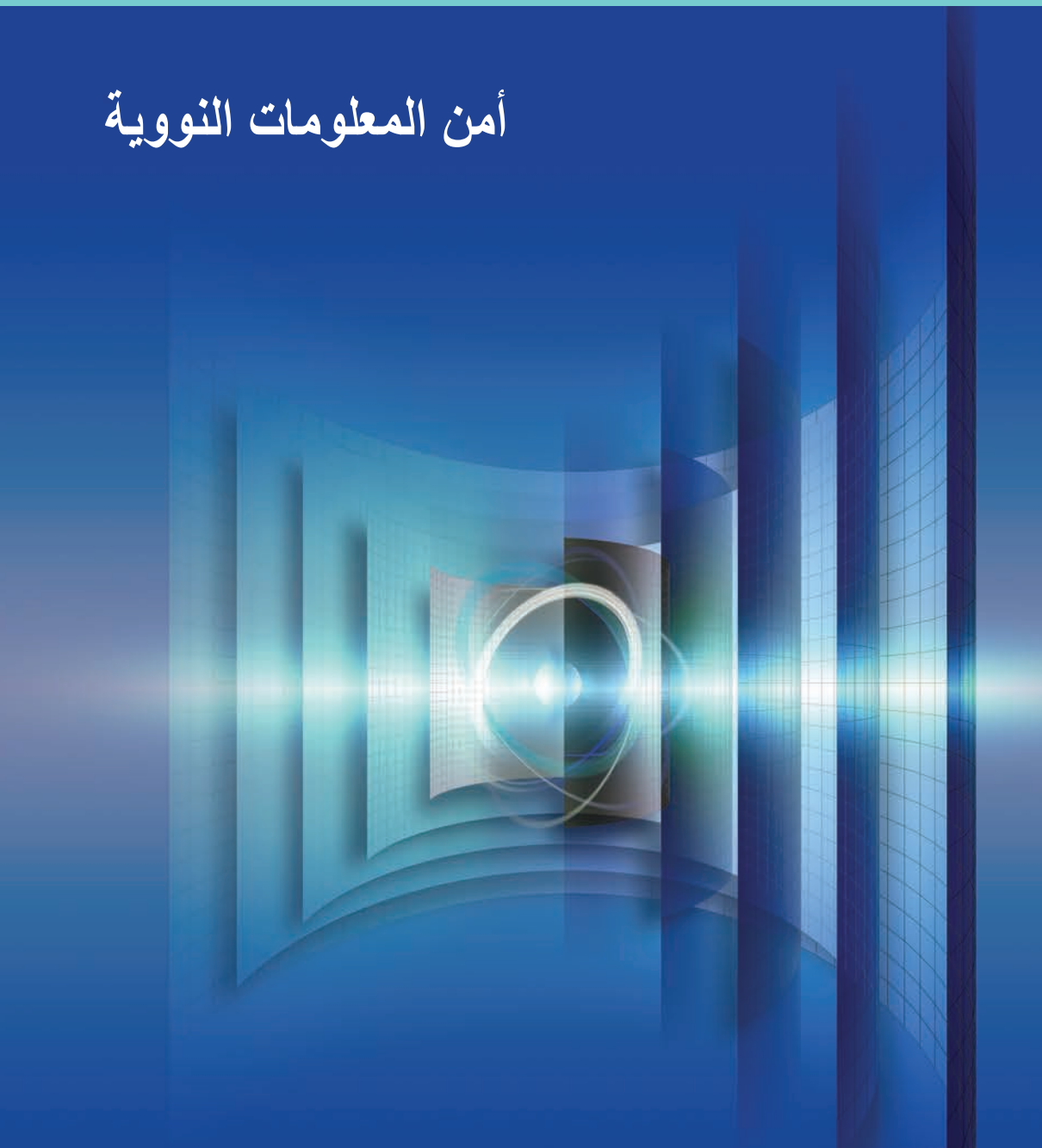
العدد G-23 من سلسلة منشورات الأمن النووي الصادرة عن الوكالة

دليل التنفيذ

أمن المعلومات النووية



IAEA
الوكالة الدولية للطاقة الذرية

سلسلة الأمن النووي الصادرة عن الوكالة

تعالج **سلسلة الأمن النووي الصادرة عن الوكالة** قضايا الأمن النووي المتعلقة بمنع وكشف الأفعال الإجرامية أو المتعمدة غير المأذون بها المنطوية على مواد نووية أو مواد مشعة أخرى أو ما يرتبط بذلك من مرافق أو أنشطة، أو المستهدفة لها، والتصدي لتلك الأفعال. وتتسق هذه المنشورات مع الصكوك الدولية المتعلقة بالأمن النووي، وتكمِّلها، مثل اتفاقية الحماية المادية للمواد النووية وتعديلها، والاتفاقية الدولية لقمع أعمال الإرهاب النووي، وقراري مجلس الأمن التابع للأمم المتحدة رقم ١٣٧٣ و١٥٤٠، ومدونة قواعد السلوك بشأن أمان المصادر المشعة وأمنها.

فئات سلسلة الأمن النووي الصادرة عن الوكالة

تصدر منشورات سلسلة الأمن النووي الصادرة عن الوكالة في الفئات التالية:

- **أساسيات الأمن النووي** التي تحدد هدف نظام أمن نووي لدولة ما والعناصر الأساسية لنظام من ذلك القبيل. وتوفر الأساس لتوصيات الأمن النووي.
- **توصيات الأمن النووي** التي تحدد التدابير التي ينبغي أن تتخذها الدول من أجل تحقيق وتعهّد نظام أمن نووي وطني فعّال يتّسق مع أساسيات الأمن النووي.
- **أدلة التنفيذ** التي تقدم إرشادات عن الوسائل التي يمكن للدول أن تنفذ من خلالها التدابير المحدّدة في توصيات الأمن النووي. وبهذا، تركِّز على كيفية العمل بالتوصيات المتعلقة بمجالات واسعة للأمن النووي.
- **الإرشادات التقنية** تقدّم إرشادات عن مواضيع تقنية محدّدة لاستكمال الإرشادات المحدّدة في أدلة التنفيذ. وهي تركِّز على تفاصيل كيفية تنفيذ التدابير الضرورية.

الصياغة والاستعراض

يشارك في إعداد منشورات سلسلة الأمن النووي واستعراضها أمانة الوكالة، وخبراء من الدول الأعضاء (الذين يساعدون الأمانة في صياغة المنشورات) ولجنة إرشادات الأمن النووي، التي تستعرض وتعتمد مسودّة المنشورات. وعند الاقتضاء، تُعقد أيضاً اجتماعات تقنية مفتوحة العضوية خلال عملية الصياغة من أجل إتاحة الفرصة للأخصائيين من الدول الأعضاء والمنظمات الدولية المعنية لاستعراض ومناقشة مسودّة النص. وإضافة إلى ذلك، ولضمان مستوى رفيع من الاستعراض وتوافق الآراء على الصعيد الدولي، تعرض الأمانة مسودّات النصوص على جميع الدول الأعضاء لفترة ١٢٠ يوماً لكي تستعرضها استعراضًا رسميًا.

وتُعِّد الأمانة لكل منشور الخطوات التالية، التي توافق عليها لجنة إرشادات الأمن النووي على مراحل متتالية ضمن عملية الإعداد والاستعراض:

- عرضًا وخطة عمل يصفان المنشور المتوخى الجديد أو المنقّح، وغرضه المستهدف ونطاقه ومحتواه؛
- مسودّة منشور لعرضها على الدول الأعضاء للتعليق عليها خلال فترة ١٢٠ يومًا الاستشارية؛
- صيغة نهائية لمسودّة المنشور مع مراعاة تعليقات الدول الأعضاء.

وتُراعى في عملية صياغة واستعراض المنشورات في سلسلة الأمن النووي الصادرة عن الوكالة اعتبارات السرية، ويسلم فيها بأن الأمن النووي يتصل اتصالاً متلازماً بشواغل الأمن الوطني العامة والمحددة.

وأحد الاعتبارات المستند إليها هو أن معايير أمان الوكالة وأنشطتها الرقابية ذات الصلة ينبغي أن توضع في الاعتبار في المضمون التقني للمنشورات. وعلى وجد التحديد، تقوم اللجان المعنية بمعايير الأمان ذات الصلة ولجنة إرشادات الأمن النووي باستعراض منشورات سلسلة الأمن النووي التي تعالج المجالات التي يوجد فيها ترابط مع الأمان المعروفة بوثائق الترابط – في كل مرحلة من المراحل المحدّدة أعلاه.

أمن
المعلومات النووية

الدول الأعضاء في الوكالة الدولية للطاقة الذرية

الاتحاد الروسي
إثيوبيا
أذربيجان
الأرجنتين
الأردن
أرمينيا
إريتريا
إسبانيا
أستراليا
إستونيا
إسرائيل
أفغانستان
إكوادور
ألبانيا
ألمانيا
الإمارات العربية المتحدة
أنتيغوا وباربودا
إندونيسيا
أنغولا
أوروغواي
أوزبكستان
أوغندا
أوكرانيا
آيرلندا
آيسلندا
إيطاليا
بابوا غينيا الجديدة
باراغواي
باكستان
بالاو
البحرين
البرازيل
بربادوس
البرتغال
بروناي دار السلام
بلجيكا
بلغاريا
بليز
بنغلاديش
بنما
بنن
بوتسوانا
بوركينا فاسو
بوروندي
البوسنة والهرسك

بولندا
بيرو
بيلاروس
تايلند
تركيا
ترينيداد وتوباغو
تشاد
توغو
تونس
جامايكا
الجبل الأسود
الجزائر
جزر البهاما
جزر مارشال
جمهورية أفريقيا الوسطى
الجمهورية التشيكية
الجمهورية الدومينيكية
الجمهورية العربية السورية
جمهورية الكونغو الديمقراطية
جمهورية إيران الإسلامية
جمهورية تنزانيا المتحدة
جمهورية فنزويلا البوليفارية
جمهورية كوريا
جمهورية لاو الديمقراطية الشعبية
جمهورية مقدونيا اليوغوسلافية سابقاً
جمهورية مولدوفا
جنوب أفريقيا
جورجيا
جيبوتي
الدانمرك
دولة بوليفيا المتعددة القوميات
دومينيكا
رواندا
رومانيا
زامبيا
زمبابوي
سان مارينو

سري لانكا
السلفادور
سلوفاكيا
سلوفينيا
سنغافورة
السنغال
سوازيلند
السودان
السويد
سويسرا
سيراليون
سيشيل
شيلي
صربيا
الصين
طاجيكستان
العراق
عُمان
غابون
غانا
غواتيمالا
غيانا
فانواتو
فرنسا
الفلبين
فنلندا
فيجي
فييت نام
قبرص
قطر
قيرغيزستان
كازاخستان
الكاميرون
الكرسي الرسولي
كرواتيا
كمبوديا
كندا
كوبا
كوت ديفوار
كوستاريكا
كولومبيا
الكونغو
الكويت
كينيا
لاتفيا

لبنان
لختنشتاين
لكسمبورغ
ليبيا
ليبيريا
ليتوانيا
ليسوتو
مالطة
مالي
ماليزيا
مدغشقر
مصر
المغرب
المكسيك
ملاوي
المملكة العربية السعودية
المملكة المتحدة لبريطانيا العظمى وآيرلندا الشمالية
منغوليا
موريتانيا
موريشيوس
موزامبيق
موناكو
ميانمار
ناميبيا
النرويج
النمسا
نيبال
النيجر
نيجيريا
نيكاراغوا
نيوزيلندا
هايتي
الهند
هندوراس
هنغاريا
هولندا
الولايات المتحدة الأمريكية
اليابان
اليمن
اليونان

وافق المؤتمر الخاص بالنظام الأساسي للوكالة الدولية للطاقة الذرية الذي عُقد في المقرّ الرئيسي للأمم المتحدة في نيويورك، في ٢٣ تشرين الأول/أكتوبر ١٩٥٦، على النظام الأساسي للوكالة الذي بدأ نفاذه في ٢٩ تموز/يوليه ١٩٥٧. ويقع المقرّ الرئيسي للوكالة في فيينا. ويتمثل هدف الوكالة الرئيسي في "تعجيل وتوسيع مساهمة الطاقة الذرية في السلام والصحة والازدهار في العالم أجمع".

العدد G-23 من سلسلة الأمن النووي الصادرة عن الوكالة

أمن
المعلومات النووية

دليل التنفيذ

الوكالة الدولية للطاقة الذرية
فيينا، ٢٠١٦

ملاحظة بشأن حقوق النشر

جميع المنشورات العلمية والتقنية الصادرة عن الوكالة محمية بموجب الاتفاقية العالمية لحقوق التأليف والنشر بصيغتها المعتمدة في عام ١٩٥٢ (برن) والمنقحة في عام ١٩٧٢ (باريس). وقد عمدت المنظمة العالمية للملكية الفكرية (جنيف) لاحقاً إلى توسيع نطاق حقوق التأليف والنشر لتشمل الملكية الفكرية الإلكترونية والفرضية. ويجب الحصول على إذن باستخدام النصوص الواردة في منشورات الوكالة بشكلها المطبوع أو الإلكتروني، استخداما كلياً أو جزئياً؛ ويخضع هذا الإذن عادة لاتفاقات متعلقة برسوم الجعالة الأدبية. ويُرحَّب بأية اقتراحات تخص الاستنساخ والترجمة لأغراض غير تجارية، وسيُنظَر فيها على أساس كل حالة على حدة. وينبغي توجيه أية استفسارات إلى قسم النشر التابع للوكالة (IAEA Publishing Section) على العنوان التالي:

Marketing and Sales Unit
Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna
Austria
fax: +43 1 2600 29302
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
http://www.iaea.org/books

طُبع من قِبَل الوكالة الدولية للطاقة الذرية في النمسا
كانون الأول/ديسمبر ٢٠١٦
STI/PUB/1677
ISBN 978–92–0–612316–4
ISSN 1816–9317

تصدير

بقلم يوكيا أمانو
المدير العام

يتمثّل الهدف الرئيسي للوكالة الدولية للطاقة الذريّة بموجب نظامها الأساسي في "تعجيل وتوسيع مساهمة الطاقة الذرية في السلام والصحة والازدهار في العالم أجمع". ويشمل عملنا منع انتشار الأسلحة النووية وضمان إتاحة التكنولوجيا النووية للأغراض السلمية في مجالات من قبيل الصحة والزراعة. ومن الضروري أن تكونَ جميع المواد النووية والموادّ المشعّة الأخرى والمرافق التي يتم فيها الاحتفاظ بهذه المواد، مُدارةً على نحو مأمون ومحميّة بشكل مناسب ضدّ الأفعال الإجرامية أو الأفعال المقصودة غير المأذون بها.

وتتحمل كل دولة على حدة المسؤولية عن الأمن النووي، غير أنّ التعاون الدولي يُعدّ عاملاً حيوياً من أجل دعم الدول في إنشاء نظم أمن نووي فعالة والحفاظ عليها. وإنّ الدور المركزي الذي تؤديه الوكالة في تيسير هذا التعاون وتقديم المساعدة إلى الدول مشهود به على نطاق واسع. ويُجسّد الدور الذي تؤديه الوكالة عضويتها الواسعة، وولايتها، وخبرتها الفريدة، وتجربتها الطويلة في مجال تقديم الدعم التقني والإرشادات المتخصصة العمليّة إلى الدول.

ومنذ عام ٢٠٠٦، قامت الوكالة بإصدار منشورات من سلسلة الأمن النووي لمساعدة الدول الأعضاء على إنشاء نظم أمن نووي وطنية فعالة. وتُكمّل هذه المنشورات الصكوك القانونية الدولية المتعلّقة بالأمن النووي مثل اتفاقية الحماية المادية للمواد النووية وتعديلها، والاتفاقية الدولية لقمع أعمال الإرهاب النووي، وقراري مجلس الأمن التابع للأمم المتحدة ١٣٧٣ و١٥٤٠ ومدونة قواعد السلوك بشأن أمان المصادر المشعة وأمنها.

ويتم وضع الإرشادات بالمشاركة النشطة من جانب خبراء من الدول الأعضاء في الوكالة بما يضمن تجسيد هذه الإرشادات توافقًا بشأن الممارسات الجيدة في مجال الأمن النووي. وتقوم لجنة إرشادات الأمن النووي التابعة للوكالة، التي تم إنشاؤها في آذار/مارس ٢٠١٢ والمتكوّنة من ممثلين عن الدول الأعضاء، باستعراض مسوّدات المنشورات ضمن سلسلة الأمن النووي والموافقة عليها أثناء وضعها.

وستواصل الوكالة الدولية للطاقة الذرية العمل مع الدول الأعضاء في الوكالة لضمان إتاحة ما تدرّه التكنولوجيا النووية السلمية من منافع من أجل تحسين صحة الناس وازدهارهم ورخائهم في جميع أنحاء العالم.

ملحوظة تحريرية

الإرشادات الواردة في سلسلة الأمن النووي الصادرة عن الوكالة هي إرشادات غير مُلزمة للدول، ولكن يجوز أن تَستَخدِم الدول الإرشادات لكي تساعدها على الوفاء بالتزاماتها بمقتضى الصكوك القانونية الدولية وعلى الاضطلاع بمسؤولياتها المتصلة بالأمن النووي داخل الدولة. وتهدف الإرشادات المعبَّر عنها بجمل تبدأ بالفعل "ينبغي" إلى عرض الممارسات الدولية الجيدة والإشارة إلى إجماع دولي بأنَّ من الضروري أن تتخذ الدول الإجراءات الموصى بها أو ما يعادل ذلك من تدابير بديلة.

ويجب أن تُفهَم المصطلحات ذات الصلة بالأمن حسب تعريفها الوارد في المنشور الذي ترد فيه، أو في الإرشادات الأعلى درجة التي يدعمها المنشور. وفي غير ذلك من الحالات، فإنَّ الكلمات تُستَخدَم بمعانيها المتعارف عليها.

ويُعتَبر التذييل جزءًا لا يتجزأ من المنشور. ويكون للمواد الواردة في أي تذييل نفس صفة المتن. وتُستَخدم المرفقات لتوفير معلومات أو تفسيرات إضافية. ولا تُعتَبر المرفقات أجزاءً لا تتجزأ من النص الرئيسي.

وعلى الرغم من توخي قدر كبير من الحرص للحفاظ على دقة المعلومات الواردة في هذا المنشور، لا تتحمل الوكالة ولا دولها الأعضاء أي مسؤولية عن العواقب التي قد تنشأ عن استخدام تلك المعلومات.

واستخدام تسميات معيَّنة لبلدان أو أقاليم لا يعني ضمنًا إصدار أي حكم من جانب الناشر، أي الوكالة، بشأن الوضع القانوني لهذه البلدان أو الأقاليم أو سلطاتها ومؤسساتها أو تعيين حدودها.

وذكر أسماء شركاتٍ أو منتجاتٍ معيَّنة (سواء مع الإشارة إلى أنها مسجّلة أو دون تلك الإشارة) لا يعني ضمنًا وجود أي نية لانتهاك حقوق الملكية، كما لا ينبغي أن يُفسَّر على أنه تأييد أو توصية من جانب الوكالة.

المحتويات

١- مقدمة

الخلفية

١-١- إنّ الهدف العام من نظام أمن نووي لدولة ما هو حماية الأشخاص والممتلكات والمجتمع والبيئة من العواقب الضارة التي تنجم عن حدث أمن نووي [١]. والجماعات أو الأفراد الذين يرغبون في التخطيط لأي فعل ضار ينطوي على مواد نووية أو مواد مشعّة أخرى أو مرافق متصلة بها، أو القيام به، قد يستفيدون من الوصول إلى المعلومات الحسّاسة. وبالتالي، ينبغي تحديد هذه المعلومات وتصنيفها وتأمينها من خلال اتخاذ التدابير المناسبة. والمعلومات الحساسة هي المعلومات، أيا كان شكلها بما فيها البرامج الحاسوبية، التي يمكن أن يؤدي كشفها أو تعديلها أو تغييرها أو تدميرها دون إذن أو منع استخدامها دون إذن إلى الإخلال بالأمن النووي.

١-٢- والسريّة* هي الخاصية المتمثّلة في عدم إتاحة المعلومات أو كشفها للأفراد أو الكيانات أو خلال العمليات، دون إذن. ولا يشمل أمن المعلومات فقط ضمان سريّة* المعلومات بل أيضًا ضمان دقتها وكمالها، (سلامتها) وإمكانية الوصول إليها واستخدامها عند الطلب (توافرها).

١-٣- وضمان أمن المعلومات الحسّاسة هو شرط مسبق مشترك بين القطاعات فيما يخص الأمن النووي، وتُعدُّ النظم والتدابير الرامية إلى تحقيق أمن المعلومات على نحو فعّال عناصرَ رئيسية بالنسبة إلى نظام أمن نووي لدولة ما.

١-٤- وأساسيات الأمن النووي [١] وكافة المنشورات الثلاثة حول توصيات الأمن النووي [٢-٤] تقرّ بأهمية تأمين المعلومات الحساسة. ويوسّع هذا الدليل التنفيذي البيانات الرفيعة المستوى الواردة في تلك المنشورات لتقديم مزيد من التفاصيل حول ما يتعيّن القيام به.

الغرض

١-٥- يقدّم هذا المنشور إرشادات بشأن تطبيق مبدأ السريّة* وبشأن الجوانب الأوسع نطاقا لأمن المعلومات. وهنالك الكثير من الإرشادات الوطنية والدولية فيما يتعلّق بوضع وإدارة أطر أمن المعلومات لشتى أنواع المعلومات، سواء أكانت في شكل إرشادات رفيعة المستوى أم في شكل معايير مفصّلة. ولا يُقصد من هذا المنشور استبدال هذه

الإرشادات. بل الهدف منه هو مساعدة الدول على سد الفجوة الموجودة بين ما هو قائم من معايير حكومية ومعايير صناعية بشأن أمن المعلومات بصفة عامّة، والمفاهيم والاعتبارات الخاصة التي تنطبق على الأمن النووي، والأحكام والشروط الخاصة القائمة عند التعامل مع المواد النووية والموادّ المشعّة الأخرى.

١-٦- والهدف من هذا المنشور هو تقديم الإرشادات بشأن:

(أ) وضع إطار فعّال لضمان سريّة* المعلومات الحسّاسة وسلامتها وتوافرها (القسم ٣)، بما يشمل التشريعات واللوائح اللازمة؛
(ب) تحديد المعلومات التي يمكن أن تعتبر حسّاسة (القسم ٤)؛
(ج) الاعتبارات المتعلّقة بتقاسم المعلومات الحساسة وكشفها (القسم ٥)؛
(د) والمبادئ التوجيهية والمنهجيات التي ينبغي توخيها لضمان السريّة* والسلامة والتوافر (القسم ٦).

النطاق

١-٧- يتناول هذا المنشور أمن المعلومات الحسّاسة فيما يتعلّق بالاستخدامات المدنية للمواد النووية والموادّ المشعّة الأخرى والمرافق ذات الصلة والأنشطة ذات الصلة. وهو يركّز على المعلومات الحسّاسة المتعلقة بالمواد والمرافق الخاضعة للتحكم الرقابي.

١-٨- ومجال الأمن النووي من حيث صلته بالمواد النووية والموادّ المشعّة الأخرى غير الخاضعة للتحكم الرقابي قد ينطوي أيضًا على معلومات حسّاسة ينبغي تأمينها. وفي مثل هذه الحالات، ينبغي تطبيق الإرشادات العامة المقدمة في هذا الدليل بقدر ما هي قابلة للتطبيق.

١-٩- والجمهور الذي يستهدفه هذا المنشور هو أي شخص تناط بعهدته مسؤولية أمن المعلومات الحسّاسة. ويشمل ذلك:

(أ) السلطات المختصة، بما في ذلك الهيئات الرقابية؛
(ب) إدارات المرافق والشركات والمنظمات الضالعة في استخدام مواد نووية أو مواد مشعّة أخرى أو خزنها أو نقلها؛
(ج) مشغلي المرافق وموظفيهم، خاصة موظفي الأمن؛

(د) المقاولين وغيرهم من الأطراف الثالثة العاملة لفائدة السلطات أو المنظمات أو مشغلي المرافق؛

(هـ) وأي كيانات أخرى قد يكون قد أتيح لها الوصول بصفة مشروعة إلى معلومات حسّاسة.

الهيكل

١-١٠- بعد هذه المقدّمة، يقدّم القسم ٢ عدّة مصطلحات ومفاهيم رئيسية سيتم استخدامها ضمن هذا المنشور بمجمله. ويصف القسم ٣ العناصر اللازمة التي تبني معًا إطارًا لأمن المعلومات الحسّاسة داخل دولة من الدول، وتتناول الأقسام ٤-٦ هذه العناصر الواحد تلو الآخر. ويعرض القسم ٤ الاعتبارات المتعلّقة بتحديد أي من المعلومات هي المعلومات الحسّاسة والتي ينبغي بالتالي تأمينها. ويتضمّن القسم ٥ الاعتبارات المتعلّقة بتقاسم المعلومات الحسّاسة وكشفها. ويصف القسم ٦ بمزيد من التفصيل الإجراءات اللازم اتخاذها على مستوى المرافق لتأمين المعلومات الحسّاسة. ويقدّم المرفق الأول مثالًا عن إطار تصنيفي. أما المرفق الثاني، فيقدّم مثالًا على مخطط تصنيف أمني للمعلومات الحسّاسة المتعلقة بالأمن النووي. ويرد في المرفق الثالث مقترح صيغة ومحتوى لبرنامج تدريب وتوعية.

٢- المفاهيم والسياق

٢-١- يوضح هذا القسم معنى بعض المصطلحات الهامّة على النحو الذي تُستخدم به في هذا المنشور. كما يقوم هذا القسم بتطبيق المفاهيم الرئيسية لأمن المعلومات في سياق الأمن النووي. وترد تعاريف مجموعة واسعة من المصطلحات ذات الصلة في مسرد المصطلحات، في نهاية هذا المنشور.

المعلومات

٢-٢- المعلومات هي المعرفة، بغض النظر عن شكل وجودها أو التعبير عنها. وهي تشمل الأفكار والمفاهيم والأحداث والعمليات والخواطر والوقائع والأنماط. ويمكن تسجيل المعلومات على مواد من قبيل الورق والأفلام والوسائط المغناطيسية أو البصرية، أو الاحتفاظ بها في نظم إلكترونية. والمعلومات يمكن أن تُمثّلَ وأن تُبلّغَ بكافة

الوسائل تقريبًا. وتوجد في المجال النووي كمية وافرة من المعلومات في أشكال عديدة. وأصول المعلومات هي المعدات أو المكونات (بما في ذلك الوسائط) التي تستخدم لخزن المعلومات أو معالجتها أو مراقبتها أو إرسالها.

٢-٣- ولأغراض التعامل والأمن، يمكن تجميع المعلومات في شكل كائنات معلومات. ويمكن تعريف هذه بصفتها كافة عناصر المعلومات التي لها قيمة بالنسبة إلى منظمة ما. وعادة ما يتضمّن كائن المعلومات مجموعة من البيانات أو المعلومات أو المعارف التي تشترك من حيث استخدامها السائد أو الغرض منها أو المخاطر المرتبطة بها أو شكل تخزينها أو إرسالها.

٢-٤- ومن المهم أن يكون مفهومًا أنَّ المعلومات الحسّاسة المتعلقة بالأمن النووي قد تكون لها قيمة (قد تختلف طبيعتها ويختلف مداها) بالنسبة إلى جميع الأطراف التالية أو أي منها:

(أ) الدولة؛
(ب) السلطات المختصة؛
(ج) مشغلو المرافق (بما في ذلك الأطراف الثالثة مثل الجهات البائعة)؛
(د) خصم محتمل (من أفراد وكيانات مُنَظّمة)؛
(هـ) الوسائط؛
(و) والجمهور.

تحديد المعلومات الحساسة وتأمينها

٢-٥- المعلومات الحسّاسة هي معلومات يمكن أن يؤدي كشفها دون إذن (أو تعديلها أو تغييرها أو تدميرها أو منع استخدامها دون إذن) إلى الإخلال بالأمن النووي أو المساعدة على ارتكاب فعل ضار ضد مرفق نووي أو منظمة عاملة في المجال النووي أو أثناء عمليات النقل. وقد تشير هذه المعلومات، على سبيل المثال، إلى الترتيبات المتعلقة بالأمن النووي في مرفق ما، أو إلى النظم والهياكل والمكونات في مرفق ما، أو إلى أماكن تواجد مواد نووية أو مواد مشعّة أخرى أو إلى تفاصيل نقلها، أو إلى التفاصيل المتعلقة بالعاملين في منظمة ما.

٢-٦- ويعدّ تحديد المعلومات التي تستوفي هذا التعريف من بين الخطوات الرئيسية في وضع برنامج لأمن المعلومات لضمان السريّة*. وترد في القسم ٤ إرشادات أكثر

تفصيلاً وشمولاً بشأن هذا الموضوع. كما ترد في المرفق الثاني أمثلة توضيحية في هذا الشأن.

٢-٧- وتأمين المعلومات الحسّاسة أمر ضروري لأن الوصول السهل إلى المعلومات غير المؤمنة بصورة ملائمة يمكن أن يساعد الخصوم على التخطيط لأفعال ضارة أو ارتكابها بدرجة من الجهد أو المخاطرة ضئيلة نسبياً. فإذا تمّ، على سبيل المثال، الحصول على خطة الحماية المادية لمرفق ما من قبل خصوم يخططون للهجوم عليه، فإنهم سيكونون على معرفة بالعقبات التي قد يواجهونها، وبحجم قوة الحراسة ومدى تسليحها وحجم قوة التصدي والتوقيت التقريبي الذي قد تستغرقه هذه القوة لكي تصل إلى الموقع. كما أنهم سيكونون على معرفة بالأهداف المهمّة داخل المرفق وبأماكن تواجدها وبتدابير الحماية الخاصة بها. وبالمثل، إذا نجح خصم ما يرغب في سرقة مواد نووية خلال النقل في الحصول على جهاز يتيح الوصول إلى معلومات مفصلة حول عملية النقل المقررة — لأن هذا الجهاز لم يتم تأمينه بصورة ملائمة — فإن الخصم يمكن أن يخطط لهجوم ما على نحو أكثر فعالية. وبالتالي، فإن حيازة الخصوم لمعلومات أو أصول معلومات من هذا القبيل من شأنها أن تزيد من احتمالات نجاحهم في تحقيق مآربهم.

٢-٨- والوصول إلى المعلومات الحسّاسة وكائنات المعلومات الحسّاسة ينبغي ألاّ يكون نطاقه أوسع مما هو لازم لتسيير أعمال منظمة ما. وهذا يعني ضمنيًا أن عملية التعميم ينبغي أن تكون مقتصرة على الأفراد المأذون لهم على نحو مناسب بالوصول إلى المعلومات، وفي الظروف التي يحتاجون فيها إلى هذه المعلومات، لا غير. وتُعدّ قاعدتا "الحاجة إلى المعرفة" و"الحاجة إلى الحيازة" أساسيتين لأمن المعلومات الحسّاسة. وينبغي الاسترشاد بهاتين القاعدتين في إدارة ومراقبة حقوق الوصول إلى المعلومات. كما ينبغي استعراض حقوق الوصول هذه دوريًا وعند الاقتضاء.

٢-٩- وضمان السريّة* يتوقّف على تطبيق تدابير الأمن على المعلومات الحساسة المختارة وأصول المعلومات الحساسة (المعدات أو المكوّنات، بما في ذلك الوسائل التي تعالج المعلومات الحساسة أو تتناولها أو تخزنها أو ترسلها) لضمان ألّا تقع بين أيدي أفراد غير مأذون لهم أو منظمات غير مأذون لها، سواء منها الخارجية أو الداخلية. وترد في المنشور المعنون Preventive and Protective Measures against Insider Threats (تدابير الوقاية والحماية من التهديدات الداخلية) [٥] إرشادات بشأن تدابير الحماية من التهديد الذي

ينشأ من مصادر داخلية. وينبغي لتدابير الأمن أن تستند إلى تحليل المخاطر. وينبغي أن يظل تحليل المخاطر هذا محدّثاً من خلال عملية استعراضات دورية.

أمن المعلومات

٢-١٠- يشير أمن المعلومات، كما هو موضح في هذا المنشور، إلى ما هو قائم من نظم أو برامج أو مجموعات قواعد معمول بها لضمان سريّة* وسلامة وتوافر المعلومات أيا كان شكلها. وهو يشمل، كحد أدنى:

(أ) أمن المعلومات التي تكون في أشكال مادية (مثل الورق والوسائط الإلكترونية)؛
(ب) أمن النظم الحاسوبية، التي يشار إليها في بعض الأحيان بأمن الحواسيب أو أمن تكنولوجيا المعلومات أو الأمن السيبراني (يمكن الاطلاع على مزيد من إرشادات الوكالة في هذا الشأن في المنشور "الأمن الحاسوبي في المرافق النووية" (Computer Security at Nuclear Facilities) [٦])؛
(ج) أمن أصول المعلومات (مثل المعدات الخاصة بخزن المعلومات ومعالجتها، ونظم وشبكات الاتصال)؛
(د) أمن المعلومات المتعلقة بالعاملين في المرافق والأطراف الثالثة (مثل المقاولين والجهات البائعة) التي يمكن أن تخلّ بأمن ما سبق ذكره؛
(هـ) وأمن المعلومات غير الملموسة (مثل المعارف).

٢-١١- وعلى الرغم من أنّ السريّة* غالباً ما لا تُخَصّ بالذكر، فإنّه ينبغي للمنظمات ضمان أن تتناول برامج أمن المعلومات لديها كافة السمات الثلاث. إذ يمكن لفقدان السلامة أو التوافر أن يؤثر سلبًا في الأمن النووي بنفس القدر الذي يؤثر به سلبًا فقدانُ السريّة*. فعلى سبيل المثال، إذا لم يتسنّ للمستخدمين المأذون لهم الوصول في الوقت المناسب إلى المعلومات اللازمة لأداء واجباتهم (فقدان التوافر)، أو إذا تم تحوير هذه المعلومات على نحو ما بغية تضليلهم (فقدان السلامة).

٢-١٢- وينبغي النظر في أمن المعلومات وتطبيقه في سياق الإطار العام للأمن. فأمن المعلومات مترابط على نحو وثيق مع مجالات الأمن الأخرى مثل الحماية المادية وأمن العاملين. وعلى سبيل المثال، يمكن أن تستخدم تدابيرُ الحماية المادية لحماية المعلومات الحسّاسة وأصول المعلومات الحسّاسة، في حين تجعل تدابيرُ السريّة* مهاجمةَ نظمِ

الحماية المادية أكثر صعوبة أو غير يقينيةٍ بالنسبة إلى الخصوم. وبما أن أي فجوات أو أوجه قصور في أي من مجالات الأمن يمكن أن تؤثر في أمن المجالات الأخرى، من الضروري اتباع نهج شامل يأخذ في الحسبان كافة المجالات معًا.

٢-١٣- كما ينبغي لأمن المعلومات أن ينظر في التوازن اللازم بين الأمن وغيره من الأهداف، بما يشمل الأمان، والانفتاح والشفافية، والجوانب التشغيلية. وترد إرشادات بشأن الأمان في سلسلة معايير الأمان الصادرة عن الوكالة.

٣- إطار لتأمين المعلومات الحساسة

٣-١- إنّ تأمين المعلومات الحسّاسة على أساس مجزأ، في كلّ مرفق على حدة، لن يكون فعالًا. وبالتالي، من الضروري إقامة إطار وطني فعال لضمان اتخاذ تدابير أمن شاملة في جميع المرافق والمواقع والمنظمات (الحكومية وغير الحكومية) التي تتعامل مع المعلومات الحسّاسة. وينبغي للدولة إرساء هذا الإطار الوطني، الذي سيشمل وضع:

(أ) مسؤولية الدولة؛
(ب) إطار قانوني ورقابي؛
(ج) الإرشادات الوطنية؛
(د) السياسات المتعلقة بالأمن؛
(هـ) ومخططات التصنيف.

كما تسهم السياسات المتبعة ضمن كلّ منظمة في الإطار العام.

المسؤوليات

٣-٢- تقع مسؤوليةُ ضمانِ وجود نظام أمن نووي شامل لدولة ما وتشغيله على نحو فعال على عاتق حكومة تلك الدولة. وضمانُ أمن المعلومات الحسّاسة جزء لا يتجزأ من نظام الأمن النووي الذي ينبغي على الدولة إنفاذه.

٣-٣- وعادة ما تكون للدول منظمات أو وكالات مسؤولة عن الأمن الوطني العام، يشار إليها فيما يلي بسلطات الأمن الوطنية. وعادة ما تتحمّل سلطات الأمن الوطنية مسؤولية تحديد السياسة الوطنية الأساسية بشأن جميع جوانب الأمن. وغالبًا ما تكون

السياسات والتعليمات المتعلّقة بالأمن الصادرة عن سلطات الأمن الوطنية ذات طابع عام، وغير مصممة خصيصًا للأمن النووي. ولكن، لدى سلطات الأمن الوطنية في عديد من الدول سياسات وإرشادات لتأمين المعلومات الحسّاسة، على سبيل المثال فيما يتعلق بالاستخدامات الحكومية أو العسكرية.

٣-٤- وينبغي للسلطات المختصَّة ذات الصلة التابعة للدولة وضع وإصدار سياسات ومتطلبات خاصّة بأمن المعلومات الحسّاسة في المرافق ذات الصلة والأنشطة ذات الصلة التي تنطوي على المواد النووية والموادّ المشعّة الأخرى. وعادة ما تكون الأخيرة مستندة إلى، أي سياسات ومتطلبات خاصة بالأمن الوطني صادرة عن سلطات الأمن الوطنية، ومتوافقة معها، غير أنها تراعي الطابع الخاص للأنشطة التي تنطوي على هذه المواد. كما ينبغي للسلطات المختصَّة الحفاظ على اتصال وثيق مع سلطات الأمن الوطنية لكي يتسنى استنباط تقييم التهديدات أو التهديد المحتاط له في التصميم، على الصعيد الوطني (لمزيد من المعلومات، انظر المنشور المعنون "إعداد وصف التهديدات المحتاط لها في التصميم واستخدامه وصيانته" (Development, Use and Maintenance of the Design Basis Threat) [٧]).

٣-٥- وينبغي لكل منظمة أن تضع سياستها الداخلية والخطط والإجراءات الخاصة بها لضمان سريّة* وسلامة وتوافر أي معلومات حساسة متعلقة بالأمن النووي تكون بحوزتها أو تتعامل معها، ولحماية أصول المعلومات الحسّاسة ذات الصلة، على نحو يمتثل للسياسة الخاصة بالأمن الوطني والقوانين والمتطلبات الوطنية ذات الصلة. كما ينبغي أن يكون جميع العاملين على وعي تام بالحاجة إلى أمن المعلومات وأن يتبعوا القواعد والإجراءات الخاصة بمنظماتهم فيما يتعلق بأمن المعلومات.

الإطار القانوني والرقابي لتأمين المعلومات الحسّاسة

٣-٦- ينبغي أن تنطبق متطلبات صون الأمن النووي ضمن حدود دولة ما على كافة الوزارات والإدارات والوكالات وغيرها من المنظمات التي تتناول قضايا ترى الدولة أنها ضرورية للأمن النووي الوطني. ويمكن للدولة أن تفرض هذه المتطلبات بواسطة القوانين أو اللوائح أو غيرها من المتطلبات الملزمة قانونًا. وينبغي أن تشمل متطلبات الدولة للأمن النووي متطلبات أمن المعلومات. كما ينبغي أن تكون هنالك تشريعات قائمة تحدّد الجزاءات أو العقوبات التي سيتم تسليطها على كل من يخرق متطلبات أمن المعلومات هذه، أيا كان، من أفراد أو منظمات. ويمكن أن تتضمّن هذه التشريعات

أقساماً تحدّد جسامة أنواع معينة من حالات خرق السريّة* أو خرق غيرها من سمات المعلومات، وما يقابلها من جزاءات.

٣-٧- وينبغي أن تكون السلطات المختصّة قادرة من خلال صلاحياتها الرقابية على فرض التزامات على من بحوزتهم معلومات حسّاسة. وينبغي للقوانين التي تم سنّها لهذا الغرض أن تنصّ على الجزاءات أو العقوبات التي يتمّ تسليطها في حالات الكشف دون إذن. كما ينبغي للجهاز التشريعي أن يُلزم وزارات الدولة وإداراتها ووكالاتها وسائر منظماتها بإمداد السلطات المختصّة بكلّ ما يلزمها من دعم لتمكينها من أداء مهمتها المتمثلة في ضمان أمن المعلومات الحسّاسة.

إعداد الإرشادات الوطنية

٣-٨- ينبغي لسياسة الدولة في مجال أمن المعلومات أن تحدّد نوع المعلومات التي تودّ الدولة تأمينها وأن تبين الكيفية التي سيتمّ بها تطبيق هذا الأمن. ويرد ذلك عادة في دليل للأمن تقوم بتجميعه سلطات الأمن الوطنية (أو السلطات المختصّة الأخرى) التابعة للدولة. ولا يجوز أن ترد في دليل من هذا القبيل أي إشارة مباشرة إلى معلومات حسّاسة بالنسبة إلى الأمن النووي. بيد أن هذا الدليل سيقوم بتحديد مختلف أصناف المعلومات مبيّناً مستوى حساسيتها وبالتالي مستوى الأمن الذي يتعيّن تطبيقه، والكيفية التي ينبغي بها وسم كائنات المعلومات لضمان أن يكون مستوى حساسيتها جليّا.

٣-٩- وينبغي للسلطات المختصة ذات الصّلة تقديم إرشادات مفصّلة بشأن ما يشكّل معلومات حسّاسة، وذلك في كنف الاتصال الوثيق مع سلطات الأمن الوطنية وبمشاركة مستخدمي المواد النووية والموادّ المشعّة الأخرى. وعادة ما تكون هذه الإرشادات مستندة إلى الأحكام الخاصة بأي تقييم للتهديدات على الصعيد الوطني، كما أنه ينبغي لهذه الإرشادات أن تكون متسقة مع الأحكام المذكورة. وإنّ هذا النوع من الإرشادات، الذي يشار إليه أحيانًا بسياسة التصنيف، عادة ما يقسم أنواع المعلومات إلى سلاسل من المواضيع ذات الصلة، ويبيّن الأهمية النسبيّة لمعلومة ما وبالتالي حساسيّتها ودرجة الأمن التي يتعيّن تطبيقها.

٣-١٠- ويمكن بيان أهمية معلومات معيّنة على مستوى المنظمة ضمن خطة الأمن الخاصة بالمنظمة، التي ينبغي أن تصف الكيفية التي ينبغي بها حماية معلومات حساسة معيّنة على نحو يمتثل للتشريعات واللوائح الوطنية.

السياسات المتعلقة بالأمن

٣-١١- بالإضافة إلى إصدار سياسات لأمن المعلومات ممتثلة للمتطلبات الوطنية، ينبغي للسلطات المختصة تقديم تفاصيل بشأن الكيفية التي يتعيّن بها تطبيق هذه المتطلبات على المرافق والأنشطة التي تنطوي على المواد النووية والموادّ المشعّة الأخرى.

٣-١٢- وينبغي أن تثبت سياسات الدولة في مجال الأمن النووي التزامها بأمن المعلومات. كما ينبغي لها أن تشجع على هذا الأمر من خلال إصدار سياسة شاملة ومناسبة لأمن المعلومات والحفاظ عليها، ليتم تطبيقها على جميع المرافق والأنشطة التي تنطوي على المواد النووية والموادّ المشعّة الأخرى، وكذلك على جميع الأماكن الأخرى حيث تُحَازُ المعلومات الحسّاسة ذات الصلة. والهدف من هذه السياسات هو ضمان أن تكون المعلومات الحسّاسة مؤمّنة ضد الإخلالات.

٣-١٣- وينبغي بعد ذلك، لأي من المنظمات والمرافق التي تتعامل مع معلومات حسّاسة أن تقوم بتجميع ما لها من سياسات مكرّسة وخاصة بها لأمن المعلومات، استنادًا إلى سياسات السلطات المختصة حيثما كان ذلك منطبقاً. وينبغي أن تُبلّغ هذه السياسات على كامل نطاق المنظمة في شكل ذي صلة ومتاح ومفهوم من قبل المستخدِمين المستهدفين. ويتضمّن القسم ٦ مزيداً من الإرشادات بشأن وضع برنامج لإدارة أمن المعلومات، بما في ذلك السياسات.

مخططات تصنيف المعلومات

٣-١٤- يحتاج تنفيذ مخططات أمن المعلومات وما يرتبط بها من ضوابط إلى الموارد والوقت. وليس من المجدي أو المرغوب فيه تأمين جميع المعلومات الموجودة في موقع ما أو مرفق ما بنفس القدر. فبعض المعلومات غير حساسة ولا تحتاج أي تدابير ضمان خاصّة. وحتى بالنسبة إلى المعلومات الحسّاسة، قد تحتاج مختلف كائنات المعلومات مستويات أمن مختلفة. ولذا، من المهم تحديد أي المعلومات هي المعلومات الحساسة، وأي مستوى من الأمن تتطلّبه. وينبغي للسلطات المختصة في كل دولة تحديد أي المعلومات المتعلّقة بالمواد النووية والموادّ المشعّة الأخرى والمرافق ذات الصلة والأنشطة ذات الصلة تشكّل معلومات حسّاسة. وفيما يتعلق بالنقل الدولي، يتعيّن على

الدولة تحديد المعلومات التي ينبغي تأمينها كما أنها قد تود أن تنظر في مدى الاتساق فيما بين الدول المشاركة في النقل الدولي.

٣-١٥- والطريقة الموصى بها لتقييم قيمة أصل معلومات معيّن هي استخدام نهج واع بالمخاطر، مع مراعاة ما من المرجّح أن يحصل من أضرار وعواقب في حال حصول إخلال بأصل المعلومات هذا. ومن المهم ملاحظة أنّ أي إخلال بالمعلومات في أحد المرافق يمكن أن يؤثّر في غيره من المرافق التي بها أصول معلومات مماثلة، وبالتالي، ينبغي النظر في الأضرار والعواقب على نطاق واسع فيما يتعلق بآثار الأمن النووي في أماكن أخرى وليس في مكان محدد واحد فقط. وينبغي إيلاء اعتبار خاص لتراكمات المعلومات ونقاط العطل الأحادية المحتملة (من قبيل أصول المعلومات المعتمدة على شبكة أحادية أو إمداد أحادي بالكهرباء). ويمكن أن تستخدم نتائج هذا التقييم لتحديد المستوى المطلوب من الأمن اللازم لكل كائن من كائنات المعلومات، وذلك وفقًا لنظام التصنيف المستخدم من قبل دولة معيّنة.

٣-١٦- وينبغي وضع نظام تصنيف وطني والحفاظ عليه بغية جمع المعلومات ضمن أصناف، على نحو تكون فيه لحالات الكشف دون إذن عن أي معلومات ضمن صنف ما نفس العواقب، وينبغي فيه بالتالي لجميع المعلومات ضمن صنف معيّن أن تكون خاضعة لنفس متطلبات الأمن. وينبغي أن يكون هذا النظام نظامًا وطنيًا، وليس خاصًا بصناعة معينة، أو من استنباط مرفق واحد. وفي العديد من الحالات، تكون الدول بالفعل محافظة على نظم تصنيف من هذا القبيل، بيد أن هذه النظم قد لا يكون الغرض منها معالجة معلومات خاصة بالأمن النووي. ويستند هذا النظام إلى نهج واع بالمخاطر، تحدد فيه العواقب المحتملة لحالات الكشف دون إذن عن المعلوماتِ صنفَ هذه المعلومات ومتطلبات الأمن ذات الصلة الخاصة بها.

٣-١٧- وينبغي النظر بعناية في عدد فئات التصنيف وفيما سيدرّه استخدامها من منافع. والعمل بالمخططات البالغة التعقيد قد يصبح أمرًا شاقًا وغير عملي، في حين أنّ المخططات البسيطة جدًا قد لا تقدم تصنيفًا دقيقًا بما فيه الكفاية. وبالإضافة إلى ذلك، ينبغي توخي الحذر عند تعيين مستوى التصنيف لكائنات المعلومات. ففرط التصنيف (أي تَطَلّبُ أمنًا أكثر صرامة مما هو حقًا ضروري) يمكن أن يؤدي إلى تكبّد نفقات إضافية غير ضرورية في حين أنّ نقصًا في التصنيف يعرّض المعلومات إلى خطر الإخلالات وهو أمر غير مقبول. كما يمكن لفرط التصنيف أن يتضارب مع السياسات

الخاصة بالشفافية أو أن يحدث وضعًا يغدو فيه التصنيف أقلّ فائدة بالنسبة إلى مستخدمي هذه المعلومات.

٣-١٨- وقد يتضمّن مخطط تصنيف محتمل للمعلومات الحساسة، بأصناف تبيّن حساسية كائنات معلومات معينة، المستويات التالية[١]:

(أ) سرّية؛
(ب) سريّة*؛
(ج) مقيّدة؛

٣-١٩- وقد تبيّن وسوم إضافية خاصة بالمعلومات ما يفرض من قيود على توزيع المعلومات نتيجة لتصنيفها، مثل:

(أ) لا مزيد من التوزيع؛
(ب) توزيع خاضع لرقابة المصدر؛
(ج) للاستخدام الرسمي؛
(د) توزيع مقيّد؛
(هـ) ومتاح للاستخدام العام؛

٣-٢٠- وترد في المرفق الأول أمثلة عن تعاريف لمستويات التصنيف من سريّة إلى مقيّدة.

٤- تحديد المعلومات الحساسة

٤-١- إن الخطوة الأولى في تصنيف وتأمين المعلومات هي تحديد المعلومات التي تعتبر معلومات حسّاسة.

٤-٢- وينبغي النظر في الضوابط الأمنية بالنسبة إلى المعلومات التي تكون من بين الأنواع التالية على الأقل، والتي يمكن أن تؤثر في الأمن النووي[٢]:

---

[١] يوجد في العديد من الدول تصنيف إضافي لمستوى **'سرية للغاية'**. ولا يستخدم مستوى التصنيف هذا تقريبًا البتة في القطاع المدني في معظم الدول. وهو ينطبق عمومًا في القطاع العسكري وقطاع الأسلحة.

[٢] لا يراد من هذه القائمة أن تشمل جميع الإمكانيات من هذا القبيل، غير أنه ينبغي لها أن تقدم منطلقًا للنظر فيها.

(أ) تفاصيل نظم الحماية المادية وأي تدابير أمن قائمة أخرى خاصة بالمواد النووية والموادّ المشعّة الأخرى والمرافق ذات الصلة والأنشطة ذات الصلة، بما في ذلك المعلومات عن قوات الحراسة وقوات التصدّي؛

(ب) معلومات عن كميّة وشكل المواد النووية أو الموادّ المشعّة الأخرى المستخدمة أو المخزّنة، بما في ذلك المعلومات المتعلّقة بحصر المواد النووية؛

(ج) معلومات متعلّقة بكمية وشكل المواد النووية أو الموادّ المشعّة الأخرى أثناء عمليات النقل؛

(د) تفاصيل النظم الحاسوبية، بما في ذلك نظم الاتصال التي تقوم بمعالجة معلومات مهمّة على نحو مباشر أو غير مباشر للأمان والأمن، أو التعامل معها أو خزنها أو إرسالها؛

(هـ) خطط الطوارئ والتصدي لحادثات الأمن النووي؛

(و) معلومات شخصية عن العاملين والجهات البائعة والمقاولين؛

(ز) معلومات عن تقييمات التهديدات والإنذار الأمني؛

(ح) تفاصيل تكنولوجيا حسّاسة؛

(ط) تفاصيل الثغرات أو مكامن الضعف المتعلقة بالمواضيع المذكورة أعلاه؛

(ي) والمعلومات التاريخية عن أي من المواضيع المذكورة أعلاه.

كما يمكن أن تخضع بعض من المعلومات الواردة أعلاه، من قبيل المعلومات الشخصية، إلى متطلبات أمن محدّدة بموجب قوانين وطنية أخرى أو سياسات شركات أخرى.

٤-٣- ويتضمّن المرفق الثاني أمثلة عن أنواع محددة من المعلومات تقع ضمن الأصناف الواردة في الفقرة ٤-٢، تبيّن ما إذا كانت هذه المعلومات تعتبر عادة معلومات حسّاسة ولماذا.

٥- تقاسم المعلومات الحساسة وكشفها

٥-١- ستكون هنالك في كثير من الأحيان حاجة مشروعة إلى تقاسم المعلومات الحسّاسة على نحو مستمر، مثلما هو الحال على سبيل المثال فيما بين الوكالات الحكومية المختصّة، أو فيما بين المنظمات التي تتعامل مع المواد النووية أو الموادّ المشعّة الأخرى والسلطات المختصَّة المعنية، أو فيما بين مختلف الدول. وبالمثل، ستكون هنالك في بعض الأحيان حاجة إلى كشف معلومات حسّاسة على أساس

مخصّص لمنظمات أخرى أو للجمهور. وينبغي أن تدار عمليات التقاسم والكشف على نحو يضمن عدم تقاسم المعلومات الحسّاسة أو كشفها، عن غير قصد، لمن هم ليسوا في حاجة إلى معرفتها.

تقاسم المعلومات

٥-٢- يكون في بعض الأحيان ضرورياً تقاسم بعض المعلومات الحسّاسة مع الوكالات أو الشركات الحكومية المأذون لها والمنظمات التي هي في حاجة إلى معرفة هذه المعلومات. فتقاسم المعلومات يمكن أن ينشئ أوجه كفاءة ما كانت لتوجد لو تم استحداث المعلومات والتعامل معها على نحو مستقلّ. كما أن هنالك حالات قد يتسبب فيها عدم تقاسم المعلومات في إلحاق الضرر بالأمن أو في إضعاف المراحل الإجمالية من تخطيط ووضع وتنفيذ لتدابير الأمن. وعلاوة على ذلك، بما أنّ المسؤوليات في مجال الأمن النووي غالبًا ما لا تكون مناطة حصريًا بعهدة وكالة واحدة أو شركة واحدة أو منظمة واحدة، يكون في كثير من الأحيان من الضروري تقاسم المعلومات بين الكيانات التي تكون لها مسؤوليات مشتركة في مجال الأمن. وعلى سبيل المثال، غالبًا ما يكون من مصلحة الأمن الوطني أن تنقل السلطات المختصّة المعلومات الحساسة إلى سلطات الأمن الوطنية والعكس صحيح، مثلما هو الحال على سبيل المثال عندما يتعيّن، في حال حصول تغييرات على تقييمات التهديدات أو معلومات عن الحادثات الأمنية، إبلاغ الأطراف المعنية بذلك في الوقت المناسب، من أجل التمكين من تعديل تدابير الأمن وتبادل التجارب التشغيلية كأساس للتحسين المتواصل. وبالإضافة إلى الاعتبارات الأمنية، يمكن أن تكون هنالك حاجة إلى تقاسم المعلومات بغية دعم أهداف أخرى، بما في ذلك تقييم الأمان والاحتياجات التشغيلية والتجارية.

٥-٣- وينبغي أن يستند طابع تقاسم هذه المعلومات ومداها إلى الامتثال إلى القوانين أو اللوائح الوطنية أولًا، ثم إلى توازن بين المنافعِ التي يدرّها التقاسم والاحتياجاتِ في مجال الأمن. كما ينبغي أن تحكم القوانين المتعلّقة بنقل المعلومات بين هذه السلطات من خلال إجراءات الأمن السارية في الدولة المعنية. ومن شأن إرساء نهج موحد ضمن أجهزة الدولة ضمان ألاّ يتم الكشف عن المعلومات الحساسة على نحو غير ملائم.

٥-٤- ومن الضروري في كثير من الأحيان تقاسم بعض المعلومات مع سائر الدول أو المنظمات الدولية ذات الصلة. وفي هذه الحالة، ينبغي أن يكون هنالك اتفاق مبرم

لضمان تأمين المعلومات الحساسة من قبل الجهة المتلقية على نحو يتفق مع متطلبات الجهة المالكة للمعلومات. ويمكن ضمان أمن المعلومات من خلال إبرام معاهدة ثنائية أو متعددة الأطراف أو اتفاق ثنائي أو متعدد الأطراف، مما يسمح بتحديد الكيفية التي يتم بها تأمين المعلومات ضد الكشف. وفي هذه الاتفاقات، عادة ما يتم وصف تدابير الحماية اللازمة التي ينبغي تطبيقها على المعلومات الحساسة بالنسبة إلى مختلف مستويات التصنيف في كل دولة. كما ينبغي لهذه الاتفاقات أن تأخذ بعين الاعتبار الكيفية التي يمكن بها للمتطلبات الخاصة بكل دولة من الدول (مثل التشريعات المتعلقة بحرية الإطِّلاع على المعلومات أنظر الفقرة ٥-٦) أن تؤثر في التعامل مع المعلومات الحساسة الخاصة بالدول الأخرى.

كشف المعلومات

الحاجة إلى الكشف

٥-٥- لدى معظم الدول قوانين سارية تتناول مسألة أمن المعلومات التي تكتسي أهمية بالنسبة إلى المصلحة الوطنية. وتحدد هذه القوانين العقوبات التي سيتم تسليطها في حال قام شخص أو مواطن أو غيرهما من تلك الدولة بخرق القوانين المتعلقة بسرية* هذه المعلومات. وعادة ما تكون هنالك قوانين تحكم وصول الأفراد إلى المعلومات الحكومية الرسمية. كما يمكن أن تكون هنالك آليات لتسوية الخلافات بين الحكومات والأطراف الأخرى فيما يتعلّق بأي معلومات يجوز الاحتفاظ بها لحماية الأمن الوطني.

٥-٦- ولدى عدة دول تشريعات متعلقة بحرية الإطِّلاع على المعلومات أو قوانين أخرى تتيح لأفراد من الجمهور طلبَ الحصول على معلومات تحتفظ بها السلطات. وعادة ما تكون المعلومات الوحيدة التي يجوز للسلطات الاحتفاظ بها معلومات من الأنواع التي تشملها إعفاءات محددة، من قبيل المعلومات المتصلة بالدفاع الوطني أو المعلومات الخاصة والشخصية. وفي عدد من الدول، لا تكون مفردة حاملة لوسم تصنيفي تلقائياً معفاة من الكشف.

٥-٧- ويمكن أن تتطلب قوانين ولوائح أخرى عدم الكشف عن أنواع معينة من المعلومات التي قد تتضمن معلومات حساسة. ومن الأمثلة عن ذلك التشريعات البيئية التي تتطلّب إبلاغ الجمهور بمعلومات محددة. وينبغي ضمان أن تسمح هذه القوانين

بإعفاء المعلومات، التي قد تؤثر في الأمن الوطني أو في أمن الأطراف الثالثة، من الكشف.

إعداد الإرشادات بشأن الكشف

٥-٨- ينبغي وضع إرشادات محددة لمساعدة المنظمات والمرافق في اتخاذ القرار بشأن أيّ من المعلومات الحساسة يمكن كشفها. وعند تجميع هذه الإرشادات، فإن الوكالة الحكومية المسؤولة عادة ما تتشاور مع غيرها من الإدارات الحكومية والمنظمات ذات الصلة. ومن خلال تحديد نوع المعلومات التي تعتبرها غير ملائمة للكشف، ينبغي للإرشادات أن تهدف إلى منع الكشف عن المعلومات الحساسة دون إذن (أنظر أيضًا المرفق الثاني).

٥-٩- وينبغي للدول النظر في الحاجة إلى تقديم إرشادات محدّدة بشأن:

(أ) حساسية بعض الأنواع من المعلومات الحساسة، استنادًا إلى عواقب الكشف عنها؛

(ب) أي أنواع من المعلومات يمكن الكشف عنها، وفي أي ظروف، ولمن وبأية أساليب محددة؛

(ج) الشروط المتعلقة بالكشف عن المعلومات؛

(د) عمليات استعراض المعلومات لتحديد حساسيتها المحتملة قبل عرضها للجمهور، مثلما هو الحال بالنسبة إلى العروض الإيضاحية في المؤتمرات، أو عمليات النشر على شبكة الإنترنت، أوالمواصفات التقنية؛

(هـ) وأي إجراءات ينبغي اتخاذها في أية حالة من حالات الكشف عن المعلومات الحساسة دون إذن، المقصودة منها أو غير المقصودة، أو غيرها من حالات خرق متطلبات أمن المعلومات.

٥-١٠- وسوف تكون هنالك حاجة إلى تعديل هذه الإرشادات. فالظروف تتطور والمعلومات التي تعتبر حساسة وغير ملائمة للكشف في وقت ما قد تكون أقل حساسية بكثير وملائمة للكشف في وقت لاحق (أو العكس). ولذلك، ينبغي استعراض الإرشادات وتحديثها دوريًا، وكذلك في حال حدوث تغييرات كبيرة في السياسات أو الظروف.

٥-١١- وخفض مستوى الأمن المطبق على معلومات معيّنة،عند الاقتضاء، سيكون عموماً مجدياً. ومع ذلك، فإنّ إعادة تصنيف المعلومات إلى صنف أكثر تقييدًا قد تكون

مستحيلة أو عديمة الفاعلية إذا ما تم الكشف عنها سابقًا على نطاق أوسع. وينبغي أن يؤخذ هذا الأمر بعين الاعتبار خلال عملية التصنيف الأصلية، كما أنه ينبغي النظر في ضمان التوازن المناسب بين السريّة* والحذر من جهة، والتوافر والشفافية من جهة أخرى. كما ينبغي وضع إطار زمني افتراضي للاستعراض الدوري للتصنيفات، ولكن، ينبغي أيضًا إجراء تغييرات عند الحاجة، كما هو الشأن على سبيل المثال إذا تغيرت الظروف بشكل كبير.

٥-١٢- وينبغي النظر في جميع ما يرد على منظمة ما من طلبات كشف عن معلومات حساسة وفقاً لنفس الإرشادات أو المعايير، كما ينبغي، عند الإمكان، أن تتم معالجة جميع هذه الطلبات من خلال مكتب مركزي واحد تابع للمنظمة. ويتمثل الأسلوب الشائع استخدامه للوصول غير الملائم للمعلومات الحساسة في تقديم طلبات متعددة إلى عديد من الأفراد أو وحدات مختلفة داخل نفس المنظمة. وإذا تمت معالجة هذه الطلبات على نحو منفصل ودونما تنسيق، قد تُقدّم إجابات مختلفة وقد يتم الكشف عن معلومات حساسة ما كانت لتنكشف بطريقة أخرى.

٦- إطار الإدارة لأغراض السريّة*

٦-١- يصف القسم ٣ الإطار العالي المستوى لتأمين المعلومات الحسّاسة. ويتناول هذا القسم بمزيد من التفصيل مكونات هذا الإطار المطلوب ضمن مرفق ما أو منظمة ما، واضعاً إياها في سياق نظام الإدارة.

٦-٢- وينبغي أن يكون هنالك نظام إدارة قائم يضع السياسات والأهداف ويمكّن من تحقيق ما يعتزم تحقيقه من أهداف على نحو كفء وفعال. وإنّ نظاماً إدارياً متكاملاً (انظر المنشور "سلسلة معايير الأمان الصادرة عن الوكالة، العدد GS-R-3، النظام الإداري للمرافق والأنشطة" [٨]
(IAEA Safety Standards Series No. GS-R-3, The Management System for Facilities and Activities)
والإرشادات المتصلة به) يُعَدُّ عنصر دعم حيوي لثقافة الأمن النووي. ويتم التحكم في عديد من الأنشطة المضطلع بها في المرافق بواسطة نظم الإدارة. وفي الأحوال المثالية، تقوم هذه النظم بدمج العناصر الخاصة بالأمن والأمان والصحة والبيئة والجودة والاقتصاد صلب عملية إدارة واحدة أو صلب مجموعة من النظم المتكاملة التي تعزز

بعضها البعض. وينبغي أن يكون أمن المعلومات مدمجا صلب نظام الإدارة القائم في المرفق أو المنظمة لضمان سريّة* المعلومات وسلامتها وتوافرها.

٦-٣- ويتوقّف ضمان سريّة* المعلومات الحساسة وسلامتها وتوافرها على التعيين الفعال للأدوار والمسؤوليات، والتصنيف لتحديد أي من المعلومات هي المعلومات الحسّاسة والتي ينبغي بالتالي تأمينها، ولمذا ينبغي تأمينها وعند أي مستوى (انظر القسم ٤)، والقرارات بشأن تأمين هذه المعلومات، وتنفيذ ما يلزم من تدابير أمن وتصدي (بما يشمل الاسترداد) إذا تم الإخلال بهذه المعلومات أو تمت سرقتها أو تم فقدانها.

٦-٤- وإطار الإدارة الموضّح في ما يلي ينطبق على جميع مستويات الإدارة في المنظمات الحائزة لمعلومات حساسة أو التي تتعامل مع معلومات من هذا القبيل.

المسؤوليات

٦-٥- تتحمل الإدارة المسؤولية العامة عن ضمان أن يكون أمن المعلومات قائمًا وفعالًا على كامل نطاق المرفق أو المنظمة بغية تأمين المعلومات الحساسة. وتقع على عاتق جميع العاملين الذين يتعاملون مع معلومات حساسة مسؤولية ضمان أمنها وفقًا للتشريعات الوطنية ذات الصلة، فضلًا عن سياسات المنظمة وإجراءاتها.

المسؤوليات المتعلقة بالإدارة

٦-٦- عادة ما تشمل المسؤوليات المتعلّقة بالإدارة ما يلي:

(أ) تحمّل المسؤولية العامة عن تأمين المعلومات الحساسة وأصول المعلومات الحساسة؛
(ب) ضمان الامتثال للقوانين واللوائح ذات الصلة؛
(ج) تعيين المسؤوليات التنظيمية في مجال الأمن؛
(د) تقديم تدريب وتعليم في مجال الأمن متسمين بالفعالية؛
(هـ) ضمان وضع سياسة فعّالة لأمن المعلومات؛
(و) توفير الموارد الكافية لتنفيذ برنامج أمن معلومات فعال؛
(ز) ضمان تطوير برنامج أمن المعلومات والخطط والإجراءات ذات الصلة؛

(ح) ضمان إدارة التغيير على نحو فعال فيما يتعلّق بالخطط والإجراءات والسياسات؛

(ط) وضمان القيام دورياً بعمليات مراجعة واستعراض وتنقيح لسياسات وإجراءات أمن المعلومات.

المسؤوليات المتعلقة بالتصنيف

٦-٧- ينبغي أن تقدم الإرشادات بشأن التصنيف الذي يتعيّن تطبيقه على كائن معلومات ما من قبل السلطات المختصة المعنية في شكل دليل للتصنيف أو دليل إرشادي. وتقوم هذه الوثيقة بجمع المعلومات عن مواضيع معيّنة كما أنها تبيّن حساسية هذه المعلومات. وينبغي للجهات التي تصدر عنها المعلومات الحساسة استخدام أدلة من هذا القبيل عند اتخاذ قرار بشأن مستوى التصنيف المناسب.

٦-٨- وما أن يتم نشر المعلومات، ينبغي لمتلقي كائن معلومات حساسة أو حائزه ألاّ يغيّر مستوى التصنيف المطبّق على هذه المعلومات دون إذن من قبل مُصدرها. ويجوز للمتلقين والحائزين لنسخ من هذه المعلومات، وينبغي لهم عند الاقتضاء، الطعن في مستوى التصنيف المطبّق. فعلى سبيل المثال، إذا تلقت السلطة المختصّة معلومات، من قبل مشغل ما، مصنفة على نحو غير صحيح بالنظر إلى القوانين المنطبقة، فإنه يتعيّن عليها إصدار تعليمات إلى المشغّل بتغيير التصنيف.

٦-٩- وفي الحالات التي تكون فيها المنظمة المُصدرة قد توقفت عن العمل، يصبح خَلَفُها هو المسؤول. وعندما يتعذر تحديد الخَلَفِ، يجوز لحائز لكائن معلومات حساسة، عند الاقتضاء، تغيير مستوى تصنيفه بعد التشاور مع السلطات المختصة المعنية.

٦-١٠- وإذا تم تغيير مستوى التصنيف المطبّق على كائن معلومات أو على نوع من كائنات المعلومات، ينبغي إلى أبعد حد ممكن إشعار جميع من يمكن أن يؤثر فيهم هذا الأمر. ويمكن أن يشمل ذلك حائزي المعلومات الحاليين والسابقين، فضلًا عن أولئك الذين قد يستخدمونها في المستقبل.

خطة الأمن

٦-١١- ينبغي أن يكون لدى جميع المنظمات التي تتعامل مع معلومات حساسة خطة للأمن. وينبغي أن تتضمن خطة الأمن هذه قسمًا مفصلًا يتناول على وجه التحديد أمن

المعلومات الحسّاسة. وينبغي أن يتمّ إبلاغ العاملين والمقاولين الذين يشتغلون لفائدة المنظمة بشأن المتطلبات ذات الصلة لخطة الأمن. فمن الضروري أن يدرك العاملون والمقاولون مسؤولياتهم في هذا الشأن.

السياسات والإجراءات المتعلقة بالأمن

خطة أمن المعلومات

٦-١٢- ينبغي أن تُدرج المسؤولية عن أمن المعلومات ضمن البنية الهرميّة للسياسات والإجراءات الخاصة بالمنظمة. وكحد أدنى، ينبغي معالجة ما يلي:

(أ) التعريف بأمن المعلومات وبيان أهدافه العامة ونطاقه وأهميته.

(ب) التعريف بالأدوار والمسؤوليات، بما في ذلك إنشاء جهة اتصال لتوجيه وإدارة أمن المعلومات.

(ج) الامتثال إلى متطلبات أمن المعلومات، بما في ذلك المتطلبات على الصعيد القانوني والرقابي والتعاقدي.

(د) وضع خطة لإدارة المخاطر بغية الحد من المخاطر إلى مستوى مقبول، تحدده الدولة، من خلال تطبيق ضوابط ملائمة استنادًا إلى نهج لتقييم المخاطر. وبالنسبة إلى مرفق نووي، ينبغي أن تتم الموافقة على خطة إدارة المخاطر من قبل سلطة مختصّة أو سلطة أخرى تعيّنها الدولة.

(هـ) الرصد والاستعراض المنتظم للترتيبات القائمة لضمان أن تظلّ معايير السياسات وإجراءاتها ذات صلة وفعّالة.

(و) متطلبات التعليم والتدريب لضمان أن يكون لدى الموظفين والمقاولين وغيرهم من العاملين وعي ملائم بشأن السياسات والإجراءات والممارسات بالقدر اللازم لأداء واجباتهم، وأنهم يدركون مسؤولياتهم إدراكًا تامًا (بما في ذلك التزاماتهم القانونية).

(ز) العواقب (أي العقوبات أو الجزاءات) فيما يتعلق بعدم الامتثال لمتطلبات أمن المعلومات أو حالات الإهمال المقصود في تأمين المعلومات الحساسة.

(ح) والوثائق المرجعية التي تدعم هذه السياسات، على سبيل المثال إجراءات أكثر تفصيلًا لأنظمة معينة أو قواعد متعلقة بالأمن ينبغي للمستخدمين الالتزام بها.

الجوانب الخاصة بالمعلومات الحساسة في خطة أمن المعلومات

٦-١٣- إضافة إلى الإشارة تحديدًا إلى تأمين المعلومات الحساسة، ينبغي للخطة أن تشمل أيضًا ما يلي:

(أ) دورة حياة المعلومات: تعريف عمليات إنشاء المعلومات الحساسة وتحديدها وتصنيفها ووسمها والتعامل معها واستخدامها وخزنها وإرسالها وإعادة تصنيفها واستنساخها وتدميرها؛

(ب) متطلبات الأمن الخاصة بالمعلومات الحساسة، مع إيلاء الاعتبار الواجب للأهداف الأمنية لسريّة* المعلومات وسلامتها وتوافرها؛

(ج) تقييد الوصول إلى المعلومات الحساسة وأصول المعلومات الحسّاسة لمن يحتاجونه لأداء واجباتهم، والذين لديهم السلطة اللازمة وتم إخضاعهم لتحقق من الجدارة بالثقة يتناسب مع مستوى تصنيف هذه المعلومات؛

(د) وإرسال المعلومات الحساسة على نحو يحد من أي خطر إخلال أو اعتراض أو تعديل أو تعطيل، دون إذن، إلى مستوى مقبول.

إجراءات التعامل مع المعلومات الحسّاسة

٦-١٤- ستنطوي إدارة المخاطر المتأتية من تهديدات سريّة* وسلامة وتوافر المعلومات على وضع تدابير مضادة فعّالة للتصدي لهذه لتهديدات. وستنطوي هذه العملية بالضرورة على توليفة من الضوابط الأمنية تُستمدُّ من مجالات أمن المعلومات والحماية المادية وأمن العاملين.

٦-١٥- ويضمن أمن العاملين، بما في ذلك عمليات التحقق من الجدارة بالثقة، أنّ أولئك الذين يستطيعون الوصول إلى المعلومات الحسّاسة يعتبرون جديرين بالثقة بالشكل المناسب من قبل الدولة للقيام بذلك. وفيما يتعلّق بالمعلومات ذات التصنيف المنخفض نسبيًا، ينبغي للمنظمة أن تقرّر ما إذا كانت هنالك حاجة إلى عمليات تحقق بالنسبة إلى الحالات التي تستدعي وصول العاملين إلى المعلومات؛ وإذا كان الأمر كذلك، قد يكون تحقّق محدود من خلفية الأفراد كافيًا. أما فيما يتعلق بالوصول إلى معلومات ذات تصنيف أعلى، ستكون هنالك حاجة إلى القيام بمجموعة شاملة من عمليات التحقق بغية تحديد الجدارة بالثقة. وينبغي أن تشمل عملية ضمان أمن العاملين إبرام اتفاق عدم كشف بين الشخص المعني والسلطة المختصّة أو المنظمة المعنية.

٦-١٦- وغالبًا ما تجمع الحماية المادية بين درجة من الوصول مدارة على نحو صارم من خلال مجال مأمون، وطبقة واحدة أو أكثر من تدابير الحماية المادية تكون أقرب إلى أصول المعلومات، مثل الأقبية وغيرها من الأماكن المأمونة. ويمكن استخدام نفس المبادئ لتوفير الحماية المادية للمعلومات وأصول المعلومات.

٦-١٧- وتشمل تدابير أمن المعلومات الضوابط التقنية والإجرائية والإدارية المطبقة على امتداد دورة حياة كائنات المعلومات، بما في ذلك إنشاءها، والتعامل معها، وخزنها، وإرسالها، واستنساخها وتدميرها. كما تشمل تدابير أمن المعلومات، من بين أمور أخرى:

(أ) التسيير الإداري بغية حوكمة أمن المعلومات والحفاظ عليه وتطويره (بما يشمل الخدمات المقدمة من قبل الأطراف الثالثة)؛

(ب) أمن الأفراد، خاصة خلال مراحل التوظيف، وبداية فترة التوظيف ونهايتها؛

(ج) الأمن المادي للمناطق التي تتواجد بها المعلومات الحساسة أو أصول المعلومات الحساسة، أو يتم فيها استخدامها أوالتعامل معها؛

(د) أمن التعامل الرقمي واليدوي مع المعلومات: أمن محطات العمل، الوقاية من الفيروسات والبرمجيات الضارة، حذف المعلومات وتدميرها، والعمليات اليدوية؛

(هـ) أمن شبكات الاتصال (الهواتف والبريد الإلكتروني وشبكة الإنترنت والشبكات الحاسوبية المحلية): السياسات، واستيقان المستخدمين، وتحديد المعدات، والفصل، وضوابط الربط والتوجيه، والرصد؛

(و) أمن المعدات: مراقبة الوصول، وتسجيل الاستخدام، وإدارة قطع الغيار، والمساندة الاحتياطية للمعدات الحاسمة، والترتيبات الخاصة بالوحدات الإحتياطية للإمداد بالطاقة، والتوثيق والصيانة، وتركيب الكابلات وأمن الوسائط؛

(ز) أمن البرامج الحاسوبية: مراقبة الوصول، تسجيل أنشطة المستخدمين والمستخدمين الخارقين، وإدارة الاحتياط، والتعاقد لأغراض الصيانة، وإدارة الإعدادات والإصدارات، واستخدام البرامج الحاسوبية القانونية المسجّلة، والاختبار لتحديد الثغرات، واختبار سلوك النظم في ظل حالات الخطأ؛

(ح) أمن استخدام نظم المعلومات: مراقبة حقوق المستخدمين، والتعرّف على المستخدمين والتحقق منهم، والربط بالخدمات، والنظم والمعدات، وإدارة

كلمات السرّ، والإشراف على الاستخدام، وقاعدة الشخصين (أي المراقبة من قبل شخصين اثنين) بالنسبة إلى العمليات الحرجة؛

(ط) التصنيف وما يقابله من إجراءات لأغراض التعامل مع المعلومات؛

(ي) وحماية الخصوصية.

٦-١٨- وينبغي أن يحكم التعامل مع المعلومات الحساسة من خلال إجراءات وفقًا لما يرد في قسم أمن المعلومات من سياسات وإرشادات خاصة بالأمن الوطني، بما يشمل أي تفسير تفرضه السلطات المختصة التابعة للدولة. كما ينبغي أن يتم وصف الحد الأدنى من معايير الأداء الخاصة بمختلف مستويات الأمن في خطة أمن المعلومات. ومنهجية التشفير المستخدمة لإرسال المعلومات إلكترونيًا هي مثال على ذلك.

نظام إدارة الحقوق

٦-١٩- ينبغي أن يكون هنالك نظام إدارة يفرض مراقبة، كيف ولماذا ومتى ينبغي أن يؤذن لحائزين ومستخدمين مُعيّنين للمعلومات الحساسة بالوصول إلى المعلومات الحساسة وأصول المعلومات الحسّاسة. وعادة ما يشمل نظام إدارة الحقوق ما يلي:

(أ) هيكلًا مُحدَّدًا للمسؤولية فيما يتعلق بإدارة الأذون؛

(ب) عمليات مُحدَّدة بشأن الوظيفة المتمثلة في تحديد من يحق له تعيين من ومن له الحق في الوصول إلى المعلومات الحساسة وأصول المعلومات الحسّاسة؛

(ج) عمليات مُحدَّدة بشأن كيفية التحقق من وظيفة إسناد الحق في الوصول ومراقبتها والإشراف عليها؛

(د) عمليات مُحدَّدة لاستبانة المدة الزمنية التي ينبغي أن تستغرقها عملية إسناد إذن بالوصول إلى المعلومات الحساسة وأصول المعلومات الحسّاسة؛

(هـ) عمليات مُحدَّدة لإلغاء الأذون بالوصول إلى المعلومات الحساسة وأصول المعلومات الحسّاسة؛

(و) عمليات مُحدَّدة للحفاظ على قابلية التتبّع الكامل لعملية إدارة الحقوق في جميع مراحل سلسلة إدارة الأذون بالوصول إلى المعلومات الحساسة وأصول المعلومات الحسّاسة.

الاستعراضات الدورية

٦-٢٠- ينبغي لسياسات الأمن وخططه وإجراءاته أن تُطَوّر وفقًا للظروف المتغيِّرة. وقد يُعَدُّ إدراج إطار زمني للاستعراض في وثيقة السياسات ذاتها وسيلةً فعَّالةً لضمان أن تظل هذه السياسات والخطط والإجراءات محدّثة. وفي حال طرأ على الظروف تغيير أساسي قد يؤدي إلى تغيير في السياسات، على سبيل المثال تغيير في التشريعات، يجوز إجراء استعراض في وقت أبكر. وينبغي أن يُطبّق هيكل الاستعراض على السياسات على جميع المستويات التي تكون فيها مسؤوليات في مجال الأمن النووي.

ثقافة الأمن

٦-٢١- يُعَدُّ تطوير ثقافة أمن نووي قوية وتعزيزها والحفاظ عليها عنصرًا أساسيًا من عناصر نظام أمن نووي. وينطبق هذا الأمر خصوصاً في مجال أمن المعلومات الذي غالبًا ما يمثّل فيه كل من الأشخاص والعمليات عاملًا رئيسيًا في تأمين المعلومات.

٦-٢٢- وكجزء من ثقافة أمن نووي فعّالة [٩]، ينبغي أن تدرك جميع المنظمات والعاملون والمقاولون بالكامل مسؤولياتهم المتعلّقة بالأمن وأهميتها. ومن الضروري أن يتلقّى العاملون والمقاولون تعليماً وتدريباً في مجال الأمن يتناسبان مع مسؤولياتهم واحتياجاتهم الفردية.

٦-٢٣- والعاملون والمقاولون الذين تكون مناطة بعهدتهم مسؤوليات محددة في مجال الأمن، وأولئك الذين يستطيعون الوصول إلى المعلومات الحساسة، وكذلك موظفو الإدارة على جميع مستويات منظمة ما، هم في حاجة إلى تلقي تدريب خاص وجلسات إحاطة فيما يتعلّق بمسؤولياتهم. ومن المهم أيضا ضمان أن تتلقّى الفئات الأخرى من العاملين، (مثل الرسل وأفراد الأمن والكتبة) التي تتعامل مع معلومات حساسة دون أن تكون بالضرورة على بيّنة بمحتوياتها، تدريبا في مجال الأمن خاصًا بمسؤولياتها.

٦-٢٤- والأحداث التدريبية بشأن أمن المعلومات التي تنظّم مرة واحدة لن تعزز على نحو وافٍ التدريبَ، وقد تسمح، على المدى الطويل بتراخي العاملين. وينبغي لجميع من يتعامل مع معلومات حساسة، بما في ذلك جميع موظفي الإدارة والعاملين والمقاولين أن يتلقوا باستمرار تدريبًا أثناء العمل وأن يحضروا دورات تنشيطية دوريّة. كما ينبغي الاحتفاظ بسجلات التدريب الرسمي الذي تلقاه واستكمله جميع العاملين والمقاولين. ومن المهم بصفة خاصة إبلاغ جميع العاملين والمقاولين المعنيين في أسرع وقت ممكن بأي

تغييرات تطرأ على القواعد والإجراءات المتعلّقة بالأمن. ويرد مقترح صيغة ومحتوى لبرنامج تدريب وتوعية في المرفق الثالث.

الترتيبات المبرمة مع الأطراف الثالثة فيما يتعلّق بأمن المعلومات

٦-٢٥- في بعض الأحيان، تحتاج السلطة المختصة أو المنظمة إلى طرف ثالث لتقديم خدمات أو سلع تنطوي على معلومات حسّاسة. وينبغي وضع هذه الترتيبات من خلال اتفاقات قانونية من قبيل رخصة أو عقد، بما في ذلك اتفاقات عدم الكشف. وقد تنطوي هذه الاتفاقات المبرمة مع أطراف ثالثة على معلومات حساسة توضع في عهدة الطرف الثالث. وبغية ضمان عدم تعريض هذه المعلومات للخطر، ينبغي أن تكون هنالك سياسات أو تشريعات وطنية سارية تشمل الترتيبات التي تنطوي على معلومات حساسة. وينبغي بعد ذلك إلزام المنظمات والمرافق المتعاقدة باتباع تلك السياسات.

٦-٢٦- وتقع مسؤولية ضمان أن تكون أي معلومات حساسة يعهد بها إلى أطراف ثالثة مؤمنة على نحو مرضي على عاتق المنظمات المتعاقدة عند التفاوض بشأن إقامة هذه العلاقات مع الأطراف الثالثة. وينبغي أن تكون تدابير الأمن القائمة لحماية المعلومات الحساسة متناسبة مع المخاطر ومتوافقة مع السياسات المذكورة.

٦-٢٧- وفي هذا السياق، ينبغي للسلطات المختصّة والمنظمات المختصّة التأكد من أنّ الأطراف الثالثة:

(أ) لديها عمليات وإجراءات خاصة بأمن المعلومات تفي على أقل تقدير بالمتطلبات الواردة في الترتيبات المتعلقة بالأمن الخاصة بالمنظمة؛

(ب) لديها جهة اتصال لتوجيه وإدارة الأمن في الشركة المتعاقدة؛

(ج) لديها نظام قائم لضمان خضوع جميع الموظفين الذين باستطاعتهم الوصول إلى المعلومات الحساسة التي تكون بحوزة الأطراف الثالثة إلى عمليات تحقق من الجدارة بالثقة عند مستوى مناسب؛

(د) تَضمنُ أنّ الوصول إلى المعلومات الحساسة وأصول المعلومات الحسّاسة يقتصر فقط على أولئك الذين لديهم الحاجة إلى المعرفة اللازمة والترخيص الأمني برفع الرقابة المناسب؛

(د) تُرسِل المعلومات على نحو متوافق مع التشريعات الوطنية والسياسات المحلية وبطريقة لا تعرض المعلومات إلى خطر الإخلالات؛

(و) تَضمنُ ألاّ يتم تقاسم المعلومات مع أطراف أو أفراد غير مأذون لهم؛

(ز) تَضمنُ أن يكون لدى جميع العاملين وعي ملائم بشأن السياسات الخاصة بالأمن وممارساتها وأنهم يدركون مسؤولياتهم إدراكًا تامًا (بما في ذلك التزاماتهم القانونية)؛

(ح) لديها إجراءات للتصدي للحادثات المتصلة بأمن المعلومات؛

(ط) وتَضمنُ أن تتم معاينة الترتيبات المتعلقة بالأمن داخل مباني الأطراف الثالثة بانتظام من قبل السلطات المختصة أو المنظمات المتعاقدة وفقاً لأحكام الاتفاقات، بغية كفالة امتثالها لمتطلبات الأمن المنصوص عليها في الاتفاقات.

عمليات التفتيش والمراجعة

٦-٢٨- من الضروري القيام بأنشطة توكيد بشكل دوري للحفاظ على برنامج لأمن المعلومات. وهنالك حاجة إلى توكيد أن تكون برامج الأمن القائمة في المنظمات الحائزة لمعلومات حساسة، بما في ذلك الأطراف الثالثة، ممتثلة في جميع جوانبها للسياسات واللوائح الوطنية. وعندما يكون ذلك منطبقًا، ينبغي أن تقوم السلطات المختصة باستعراض تدابير أمن المعلومات قبل منح الموافقة الرسمية باستخدامها. ويمكن تحقيق التوكيد من خلال عمليات التفتيش الرسمية المنتظمة، أو من خلال عمليات المراجعة الرسمية المنتظمة للمنظمات أو المرافق. وعادة ما تتم عمليات المراجعة داخل المنظمات في حين أن عمليات التفتيش تتم داخل المنظمات وخارجها. وبالإضافة إلى ذلك، يمكن أن تكون عمليات التفتيش معلنًا عنها أو غير معلن عنها (أي بإخطار مسبق أو دون إخطار مسبق).

٦-٢٩- وعمليات التفتيش والمراجعة الداخلية هي العمليات التي تضطلع بها المنظمة لتحديد ما إذا كان برنامج الأمن القائم ممتثلًا لخطة أمن المعلومات المعتمدة، ولضمان امتثاله للمتطلبات الرقابية. وتتيح عمليات التفتيش هذه للمنظمة التحقق من مستوى امتثال برامجها بوتيرة أكبر من تلك التي تتيحها عمليات التفتيش الخارجية. وبالإضافة إلى ذلك، فإن عمليات التفتيش أو المراجعة التي يجريها عاملون ملمّون بالمتطلبات والإجراءات والنظم الداخلية قد تؤدي إلى تحديد فرص للتحسين تختلف عن تلك التي يمكن أن تُكتشف من خلال عمليات تفتيش خارجية.

٦-٣٠- وعمليات التفتيش الخارجية هي العمليات التي تقوم بإجراءها السلطات المختصة أو غيرها من المنظمات الخارجية المأذون لها. والهدف من عمليات التفتيش هذه هو تقييم مستوى امتثال هذه السلطات أو المنظمات لسياسة أمن المعلومات الخاصة بدولة ما. وتقدم عمليات التفتيش الخارجية تقييمًا مستقلًا مقارنة بما تقدمه عمليات

التفتيش التي تقوم بإجرائها المنظمة نفسها. وعند استعمال خدمات المراجعين الخارجيين، ينبغي التطرق إلى مسائل السريّة* والجدارة بالثقة.

٦-٣١- وينبغي لعمليات التفتيش والمراجعة أن تسلّط الضوء على مجالات محددة لاتخاذ إجراءات بشأنها أو تحسينها. وينبغي وضع أطر زمنية محدّدة لما يتم استبانته من إجراءات وقائية أو تصحيحية بغية تصويبها أو تنفيذها. وينبغي أن تتم متابعة الإجراءات التصويبية والتنفيذية كما ينبغي تقييم فعاليتها.

الحادثات المتصلة بأمن المعلومات

٦-٣٢- يمكن أن تكون عمليات خرق الأمن ناتجة عن الإخلال بكائن معلومات ما. ونوعا الخرق الذي يقع فيهما الإخلال بالمعلومات هما التسريبات وحالات الفقدان. وعادة ما تكون التسريبات مقترنة بحالة إخلال بالسريّة* يحصل فيها كشف متعمّد أو عرضي عن معلومات دون إذن. أما حالات الفقدان، فعادة ما تكون مقترنة بإخلال بالمعلومات ناجم عن سرقة معلومات أو أصول معلومات، أو عن إخفاق في تأمينها على نحو مناسب.

٦-٣٣- وقد تنطوي الحادثات المتصلة بأمن المعلومات أيضًا على فقدان توافر أو سلامة المعلومات، الذي يكون بدوره ناجماً عن أفعال غير مقصودة أو مقصودة. وقد يحصل فقدان التوافر، على سبيل المثال، جراء خطأ في نظام المعلومات (خطأ في قاعدة بيانات على سبيل المثال) أو حالة منع استخدام ضارة (التشويش المتعمد لشبكة معلومات ما من خلال تسليط حركة مفرطة للبيانات). أما فقدان السلامة، فقد يكون ناتجًا، على سبيل المثال، عن ضرر يلحق بنظام المعلومات، أو إخلال بقاعدة بيانات ما، أو تغيير للمعلومات دون إذن خلال إرسالها.

٦-٣٤- وينبغي أن يكون تقديم تقارير إلى السلطات المختصة بشأن كبرى حادثات أو عمليات خرق الأمن النووي، بما في ذلك حالات خرق أمن المعلومات، إلزامياً. كما ينبغي أن يكون هذا الشرط مضمّنا في قوانين ولوائح الدولة. وينبغي لهذه القوانين أو اللوائح أن تحدّد العقوبات أو الجزاءات التي سيتم تسليطها في حال عدم تقديم هذه التقارير.

٦-٣٥- وينبغي لرؤساء المنظمات والمرافق ضمان أن تكون هنالك ترتيبات قائمة بشأن الإبلاغ الرسمي بغية كفالة أن يتم استرعاء انتباههم على نحو عاجل بشأن جميع

الحادثات المتصلة بأمن المعلومات لكي يتسنى اتخاذ إجراءات تصحيحية، وإرسال تقارير بشأن هذه الحادثات، عند الاقتضاء، إلى السلطات المختصّة. ولا ينبغي أن يشكل عامل الإحراج سبباً في عدم الإبلاغ بشأن أيّ حادثة متصلة بأمن المعلومات على أيٍّ مستوى. كما ينبغي أن يتم الإبلاغ بشأن الحادثات على وجه السرعة حتى يتسنى اتخاذ الإجراءات التصحيحية المناسبة وتحديد الاتجاهات في هذا الشأن.

عمليات التحقيق

٦-٣٦- ينبغي التحقيق في جميع الحادثات المتصلة بأمن المعلومات. كما ينبغي وضع سياسات وإجراءات تحكم عمليات التحقيق في الحادثات المتصلة بأمن المعلومات. وينبغي لعملية التحقيق أن تهدف إلى تحديد ما إذا كان لحادثة أمنية ما أثر كبير أو طفيف في أمن المعلومات وسريتها*. ويجوز بعد ذلك للسلطات المختصّة الشروع في أي إجراءات تراها مناسبة. ويمكن أن يُعتبر الإخفاق في حفظ وثيقة أو تأمينها على نحو مناسب مثالًا عن حادثة طفيفة لم ينتج عنها فقدان لأي معلومات أو إخلال بها. ويمكن أن تُعتبر سرقة خطة للأمن مثالًا عن حادثة كبيرة ينتج عنها تهديد استراتيجي لمنظمة ما.

٦-٣٧- وعند إجراء تحقيق ينبغي:

(أ) النظر بشكل كامل في ظروف الحادثة لتحديد نطاقها وحجمها وأثرها.
(ب) تقييم عواقب الحادثة ودرجة الإخلال الذي يمكن أن يكون قد حصل.
(ج) تقييم الحاجة إلى اتخاذ مزيد من الإجراءات أو القيام بتحقيقات أوسع نطاقًا، يمكن أن تشمل وكالات أخرى.
(د) التوصية باتخاذ إجراءات تصحيحية أو اتخاذ إجراءات لاحتواء العواقب أو التقليل من تبعاتها.
(هـ) الإبلاغ بشأن نتائج التحقيق، بما في ذلك:
'١' الأسباب المرجحة لوقوع الحادثة؛
'٢' درجة الإخلال التي تم تقييمها؛
'٣' الآثار التي يُرجّحُ أن تترتّب عن هذا الإخلال؛
'٤' تقديم ما يمكن من توصيات بشأن التحسينات الممكن إدخالها على برنامج الأمن لتفادي وقوع حادثات مماثلة؛
'٥' ما تقتضيه الحادثة من إجراءات أخرى يوصى باتخاذها.
'٦' والدروس التي يتعيّن استخلاصها من قبل الأطراف المعنية.

٦-٣٨- وينبغي للسلطات المختصة أن تحتفظ بسجلات بعدد وأنواع الحادثات المتصلة بأمن المعلومات التي تم الإبلاغ بشأنها. وينبغي تحديد الحادثات أو الاتجاهات المتكررة فيما يتعلق بالإخفاقات الأمنية، كما أنّ هذه الحادثات أو الاتجاهات قد تبيّن الحاجة إلى إحداث تغييرات في سياسات الأمن أو إدخال تحسينات على إجراءات الأمن أو برامجه. وينبغي أن يتضمّن التدريب في مجال التوعية تحديثات بشأن الاتجاهات والتغييرات في هذا الصدد لكي يتسنى الحفاظ على ثقافة أمن مناسبة في أوساط العاملين والمقاولين. وينبغي للمنظمات والمرافق أيضًا الحفاظ على السجلات الخاصة بها.

المراجع

[١] الوكالة الدولية للطاقة الذرية، الهدف والعناصر الأساسية لمنظومة الأمن النووي الخاصة بالدولة، العدد ٢٠ من سلسلة الأمن النووي الصادرة عن الوكالة، الوكالة الدولية للطاقة الذرية، فيينا (٢٠١٤).

[٢] الوكالة الدولية للطاقة الذرية، توصيات الأمن النووي بشأن الحماية المادية للمواد النووية والمرافق النووية (INFCIRC/225/Revision 5)، العدد ١٣ من سلسلة الأمن النووي الصادرة عن الوكالة، الوكالة الدولية للطاقة الذرية، فيينا (٢٠١١).

[٣] الوكالة الدولية للطاقة الذرية، توصيات الأمن النووي بشأن المواد المشعة والمرافق ذات الصلة، العدد ١٤ من سلسلة الأمن النووي الصادرة عن الوكالة، الوكالة الدولية للطاقة الذرية، فيينا (٢٠١١).

[٤] مكتب الشرطة الأوروبي (اليوروبول)، والوكالة الدولية للطاقة الذرية، ومنظمة الطيران المدني الدولي (إيكاو)، والمنظمة الدولية للشرطة الجنائية (الإنتربول)، ومعهد الأمم المتحدة الأقاليمي لبحوث الجريمة والعدالة، ومكتب الأمم المتحدة المعني بالمخدرات والجريمة، ومنظمة الجمارك العالمية، توصيات الأمن النووي بشأن المواد النووية والمواد المشعة الأخرى الخارجة عن التحكم الرقابي، العدد ١٥ من سلسلة الأمن النووي الصادرة عن الوكالة، الوكالة الدولية للطاقة الذرية، فيينا (٢٠١٢).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8, IAEA, Vienna (2008).

[٦] الوكالة الدولية للطاقة الذرية، الأمن الحاسوبي في المرافق النووية، العدد ١٧ من سلسلة الأمن النووي الصادرة عن الوكالة، الوكالة الدولية للطاقة الذرية، فيينا (٢٠١٣).

[٧] الوكالة الدولية للطاقة الذرية، إعداد وصف التهديدات المحتاط لها في التصميم واستخدامه وصيانته، العدد ١٠ من سلسلة الأمن النووي الصادرة عن الوكالة، الوكالة الدولية للطاقة الذرية، فيينا (٢٠١٢).

[٨] الوكالة الدولية للطاقة الذرية، النظام الإداري للمرافق والأنشطة، سلسلة معايير الأمان الصادرة عن الوكالة، العدد GS-R-3، الوكالة الدولية للطاقة الذرية، فيينا (٢٠١١).

[٩] الوكالة الدولية للطاقة الذرية، ثقافة الأمن النووي، العدد ٧ من سلسلة الأمن النووي الصادرة عن الوكالة، الوكالة الدولية للطاقة الذرية، فيينا (٢٠١١).

المرفق الأول

نظام التصنيف والتعاريف

أولاً-١- يقدّم المرفق الأول مثالاً عن إطار تصنيفي. ويجوز لفرادى الدول استنباط واستخدام أي نظام تصنيف مناسب لبيان مستوى حساسية المعلومات المتعلّقة بالأمن النووي. وتمثّل التعاريف الواردة في ما يلي نظاما من أربعة مستويات مماثلا للأنظمة المستخدمة في العديد من الدول الأعضاء. ولا تتم مناقشة المستوى الرابع سريّة للغاية إذ إنّ التجربة أثبتت أنّه من المستبعد جدًا في المجال النووي المدني أن تجتذب أي أصول معلومات التصنيفَ سريّة للغاية. وتجدر أيضاً ملاحظة أنّه، في حين أنّ المعلومات تُرتأى في المقام الأول على أنّها تأتي في شكل وثائق أو معارف، فإنّه بالإمكان تصنيف مفردات المعدات أو الكائنات المادية الأخرى عندما يتسنّى استخلاص معلومات مصنفة منها، وذلك من خلال المراقبة البصرية لمظهرها الداخلي أو الخارجي أو هيكلها أو طريقة تشغيلها أو اختبارها أو تطبيقها أو استخدامها.

المعلومات السرّية

أولاً-٢- من المرجح أن يؤدي الإخلال بالمعلومات أو المواد المصنفة سريّة إلى ما يلي:

(أ) زيادة التوتر الدولي؛
(ب) إلحاق ضرر جسيم بالعلاقات بين الحكومات؛
(ج) تهديد الحياة بشكل مباشر، أو المساس بشكل خطير بالنظام العام أو الأمن الفردي أو الحرية الفردية؛
(د) إلحاق ضرر جسيم بالفعالية التشغيلية لقوات الأمن الوطنية أو أمنها أو بالفعالية المستمرّة للعمليات الأمنية أو الاستخباراتية ذات القيمة العالية؛
(هـ) التسبب في أضرار مادية كبيرة للشؤون المالية الوطنية أو المصالح الاقتصادية والتجارية؛
(و) الاستفادة منها من قبل أفراد أو جماعات يخططون لارتكاب فعل ضار يمكن أن يتسبب في أضرار جسيمة في مرفق ذي صلة بالمواد النووية أو الموادّ المشعّة الأخرى، أوخلال نقلها.

المعلومات السريّة*

أولاً-٣- من المرجح أن يؤدي الإخلال بالمعلومات أو المواد المصنفة سريّة* إلى ما يلي:

(أ) توتير العلاقات الديبلوماسية؛
(ب) المسّ بالأمن الفردي أو الحرية الفردية؛
(ج) إلحاق ضرر بالفعالية التشغيلية لقوات الأمن الوطنية أو أمنها أو بفعالية العمليات الأمنية أو الاستخباراتية ذات القيمة العالية؛
(د) إعاقة الشؤون المالية الوطنية أو المصالح الاقتصادية والتجارية إلى حدّ كبير؛
(هـ) تقويض القدرة المالية للمنظمات الرئيسية إلى حد كبير؛
(و) عرقلة التحقيق أو تسهيل ارتكاب جرائم خطيرة؛
(ز) عرقلة وضع وتنفيذ السياسات الحكومية الرئيسية على نحو خطير؛
(ح) إيقاف كبرى العمليات الوطنية أو تعطيلها بطرق أخرى إلى حدّ كبير؛
(ط) الاستفادة منها من قبل أفراد أو جماعات يخططون لارتكاب فعل ضار يمكن أن يتسبب في أضرار جسيمة في مرفق ذي صلة بالمواد النووية أو الموادّ المشعّة الأخرى، أو خلال نقلها.

المعلومات المقيّدة

أولاً-٤- من المرجح أن يؤدي الإخلال بالمعلومات أو المواد المصنفة مقيّدة إلى ما يلي:

(أ) التأثير سلبا في العلاقات الديبلوماسية؛
(ب) التسبب في أضرار كبيرة بالنسبة إلى الأفراد؛
(ج) الزيادة من صعوبة الحفاظ على الفعالية التشغيلية لقوات الأمن الوطنية أو أمنها؛
(د) التسبب في خسائر مالية أو خسائر في الأرباح المحتملة للأفراد أو الشركات، أو في تسهيل تحقيقهم لمكاسب أو منافع على وجه غير سليم؛
(هـ) المسّ من سلامة عمليات التحقيق في الجرائم؛
(و) تسهيل ارتكاب الجرائم؛
(ز) خرق التدابير المناسبة بالحفاظ على سريّة* المعلومات المقدّمة من قبل الأطراف الثالثة؛
(ح) عرقلة العملية الفعّالة لوضع وتنفيذ السياسات الحكومية؛
(ط) خرق القيود القانونية المفروضة على الكشف عن المعلومات؛

(ي) إعاقة الحكومات فيما يتعلّق بإجراء المفاوضات التجارية أو السياسية مع الجهات الأخرى؛
(ك) تقويض الإدارة السليمة للقطاع العام وعملياته؛
(ل) الاستفادة منها من قبل أفراد أو جماعات يخططون لارتكاب فعل ضار يمكن أن يتسبب في أضرار جسيمة في مرفق ذي صلة بالمواد النووية أو الموادّ المشعّة الأخرى، أو خلال نقلها.

أولاً-٥- فيما يتعلّق بتطبيق مستويات التصنيف الواردة أعلاه على عملية مراقبة المعلومات الحسّاسة في المجال النووي، ينبغي النظر في الكيفية التي يمكن بها الكشف عن هذه المعلومات دون إذن أن يساعد خصما محتملا في ما يلي:

(أ) تحديد هدف لأعمال سرقة أو تخريب لمعدات أو مرافق ذات صلة بالمواد النووية أو الموادّ المشعّة الأخرى.
(ب) التخطيط لأعمال سرقة أو تخريب لمعدات أو مرافق ذات صلة بالمواد النووية أو الموادّ المشعّة الأخرى، أو ارتكابها مثل:
'١' تصاميم نظم الأمن؛
'٢' مخططات المباني؛
'٣' أساليب وإجراءات نقل المواد النووية أو الموادّ المشعّة الأخرى، وحصرها والتعامل معها؛
'٤' وخطط الأمن وإجراءاته وقدراته.
(ج) قياس مدى نجاح أعمال سرقة أو تخريب لمعدات أو مرافق ذات صلة بالمواد النووية أو الموادّ المشعّة الأخرى:
'١' العواقب الفعلية أو الافتراضية لتخريب معدات أو مرافق حيويّة محدّدة.
(د) الإنتاج غير المشروع لجهاز نووي متفجر، أو لجهاز نشر إشعاعات، أو لجهاز تعرض إشعاعي:
'١' المعلومات التصميمية المفيدة في تطوير جهاز ما؛
'٢' مكان تواجد المواد اللازمة لصنع جهاز ما؛
'٣' ومكان تواجد سلاح نووي.
(هـ) نشر المواد النووية أو الموادّ المشعّة الأخرى في البيئة:
'١' مكان تواجد المواد وشكلها وكميتها.

المرفق الثاني

أمثلة على معلومات حسّاسة

ثانياً-١- يقدّم المرفق الثاني مثالاً على مخطط تصنيف أمني للمعلومات الحسّاسة المتعلقة بالأمن النووي. وينبغي للدولة أن تقرر المستوى الدقيق للتصنيف الذي ينبغي تطبيقه على كل مفردة من مفردات هذه المعلومات. ويقدّم الجدول ثانياً-١ أمثلة عن معلومات حساسة كما أنه يحدد قضايا الحساسية المتصلة بها. وحيثما لا يُنصح بنشر المعلومات، يشير الجدول إلى أسباب ذلك وإلى ما إذا كان يجوز تطبيق الأمن.

ثانياً-٢- وأصناف المعلومات على النحو الوارد في الجدول ثانيا-١ توضح فقط ما يمكن اعتباره معلومات حساسة. ولا يقصد منها أن تكون قائمة شاملة أو أنموذجا شاملا. وسيتم تحديد أهمية الأصناف التي سينظر في إدراجها صلب أي جدول وطني مماثل وفقا لتقييم محدد تقوم به الدولة.

ثانياً-٣- وضمن كل خانة من الجدول، يرد في العمود الأول وصف لمثال عن نوع من أنواع المعلومات ويُبيّن العمود الثاني ما إذا كان هذا الصنف منطبقا في العادة على المواد النووية والمرافق النووية (N)، أو على الموادّ المشعّة الأخرى والمرافق ذات الصلة (R)، أو على كليهما (N, R). ويبيّن العمود الثالث ما إذا كانت المعلومات تعتبر حساسة أو غير حساسة. ويقدم العمود الأخير بعض التفسيرات لحساسية المعلومات وللأساس المنطقي لتأمينها.

ثانياً-٤- وفيما يتعلق بتصنيف المعلومات على أنها حساسة وبإسناد مستوى تصنيف محتمل، ينبغي النظر في المعلومات التي ظهرت بالفعل في المجال العام، أو في أي إخلال سابق أو إخلال محتمل بالمعلومات. فإسناد وإدارة مستوى تصنيف لمعلومات من هذا القبيل قد يكون غير عملي.

ثانياً-٥- كما ينبغي النظر في تصنيف المعلومات غير الحساسة على أنها حساسة إذا كان استخدامها يمكّن، بالاقتران مع غيرها من المعلومات غير الحساسة، من الكشف عن معلومات حساسة.

الجدول ثانياً-١- مخطط تصنيف أمني افتراضي للمعلومات الحسّاسة المتعلقة بالأمن النووي

الصنف	المجال	الحساسيّة	الأساس المنطقي للتأمين
١- أمن المواد والمرافق			
١-١- اللوائح والإرشادات			
ألف- لوائح أمن وطنية تحكم استخدام المواد النووية أو الموادّ المشعّة الأخرى	N, R	غير حسّاسة	عادة ما يتم نشر هذه المعلومات في المجال العام.
باء- إرشادات بشأن هذه اللوائح، تقوم بإصدارها السلطة المختصة أو وكالات حكومية أخرى	N, R	حسّاسة	على الرغم من أنّ جميع الإرشادات من هذا القبيل قد لا تكون حساسة، فإنّ وثيقة من هذا الطابع يمكن أن تتضمّن تفاصيل عن المعايير، وأنواع المعدات المزمع استخدامها، والإجراءات والعمليات الأمنية في مرفق ما. ويمكن لهذه التفاصيل أن تكون مفيدة لخصوم يخططون لارتكاب فعل ضار.
١-٢- سياسات الأمن النووي الوطني			
ألف- سياسات حكومية عامة بشأن المسائل التي تنطوي على المواد النووية أو الموادّ المشعّة الأخرى.	N, R	غير حسّاسة	عادة ما تكون هذه المعلومات منشورة في المجال العام.
باء- سياسات مفصلة تشمل مواضيع محددة متعلّقة بالأمن	N, R	حسّاسة	ربما تُبيّن نوع العقبات التي قد يواجهها الخصوم، مما يتيح لهم الفرصة للتخطيط للحصول على معلومات أكثر تفصيلاً.
١-٣- خطة أمن المرافق	N, R	حسّاسة	عادة ما تتضمن معلومات من هذا القبيل وصفا مفصلا لتدابير الأمن القائمة في موقع ما وتفاصيل دقيقة عن أماكن خزن المواد داخل هذا الموقع. وفيما يتعلّق بالمرافق النووية، فإنّ هذه المخططات تتضمن أيضاً تفاصيل عن المناطق الأساسية لتشغيل الموقع.

الجدول ثانياً-١- مخطط تصنيف أمني افتراضي للمعلومات الحسّاسة المتعلقة بالأمن النووي (تابع)

الصنف	المجال	الحساسيّة	الأساس المنطقي للتأمين
١-٤- التقارير المتعلقة بالأمن			
ألف- تقارير مشتقّة من الدراسات الاستقصائية الأمنية، وعمليات التفتيش الأمني، وعمليات التقييم الأمني، وغيرها من التدابير المتعلقة بالحماية المادية أو الأمن التقني المستخدمة في موقع ما أو مرفق ما	N, R	حسّاسة	الوصول إلى هذه التقارير يمكن أن يُمدّ للخصوم بتفاصيل عن مكان تواجد المواد، وعن التدابير المتخذة لحمايتها، وعمّا قد يوجد من ثغرات تم تقييمها، مما يساعدهم بالتالي على تفادي تدابير الأمن والضوابط الأمنية.
باء- تقارير تصف السمات الحرجة و/أو تسلط الضوء على متطلبات التحسين في مجال الأمن، بما في ذلك في المناطق الحيوية (إن وجدت)	N, R	حسّاسة	معلومات من هذا الطابع يمكن أن تُفيد خصوما يرغبون في تفادي الترتيبات المتعلقة بالأمن كما أنه يمكنها أن تساعدهم على استهداف مرفق.
جيم- نتائج تحقيقات أمنية في موقع ما أو مرفق ما، بما يشمل التحقيقات بشأن تسريبات المعلومات الحساسة وحالات فقدانها	N, R	حسّاسة	معلومات من هذا الطابع يمكن أن تُفيد خصوما يرغبون في تفادي الترتيبات المتعلقة بالأمن كما أنه يمكنها أن تساعدهم على استهداف مرفق ما.
دال- تقارير تصف ثغرات نظام إدارة الأمن وعواقب إصابته بالعطل	N, R	حسّاسة	معلومات من هذا الطابع يمكن أن تُفيد خصوما يرغبون في إغفال الترتيبات المتعلقة بالأمن.

الجدول ثانياً-١- مخطط تصنيف أمني افتراضي للمعلومات الحسّاسة المتعلقة بالأمن النووي (تابع)

الصنف	المجال	الحساسيّة	الأساس المنطقي للتأمين
١-٥- تفاصيل التشييد			
ألف- تفاصيل تشييد وتوضيع الأماكن التي يمكن أن يقع فيها خزن أو معالجة المواد، بما في ذلك الرسومات أو المخططات التي تكون مخزنة على أي نوع من الوسائط، والتي تُظهر سمات خاصّة بالحماية المادية تكون ذات صلة بمنع ارتكاب أفعال ضارّة	N, R	حسّاسة	يمكن نشر الخرائط الرسمية والمخططات الرسمية والمسارات الرسمية للمواقع رهناً بما تستنسبه إدارات المواقع، شريطة ألا يتضمّن ما يتم نشرهُ تَفَاصيلَ عن وظائف المباني، والمواد المخزنة فيها، والأماكن التي تتواجد فيها الأسوار الخاصة بالأمن الداخلي وغيرها من تدابير الأمن المتخذة في هذه المباني.
باء- تفاصيل تشييد المناطق الحيوية في محطات القوى النووية والمرافق النووية الأخرى	N	حسّاسة	معلومات من هذا الطابع يُمكن أن تُفيد خصوما في تفادي الترتيبات المتعلقة بالأمن كما أنه يمكنها أن تساعدهم على الاستهداف لأغراض التخريب.
١-٦- نظم الحماية			
ألف- تفاصيل عن أي تدابير من تدابير الحماية المادية المتخذة مثل أجهزة الإنذار، وكاميرات المراقبة، وضوابط الوصول، وأفراد الأمن، وما إلى ذلك.	N, R	حسّاسة	
باء- أنواع وأماكن تواجد أجهزة استشعار نظم كشف الاقتحام وما يرتبط بها من كاميرات مراقبة، بما في ذلك مخططات الدارات، وأماكن تواجد الوحدات الحاسمة للإمداد بالطاقة، وأطوال الكوابل، وبرامج الصيانة والاختبارات بالنسبة إلى هذه المعدات.	N, R	حسّاسة	من شأن أي تفاصيل من هذا الطابع أن تفيد أي خصوم يرغبون في التغلّب على نظم الأمن في مرفق.

الجدول ثانياً-١- مخطط تصنيف أمني افتراضي للمعلومات الحسّاسة المتعلقة بالأمن النووي (تابع)

الصنف	المجال	الحساسيّة	الأساس المنطقي للتأمين
١-٧- تفاصيل عن النظم المؤتمتة لمراقبة الوصول، بما يشمل أماكن تواجد خوادم الحواسيب والخوادم الاحتياطية ووحدات إمدادها بالطاقة	N, R	حسّاسة	ينبغي عدم نشر أي تفاصيل يمكن أن تؤدي إلى التغلّب على نظم مراقبة الوصول من قبل خصم داخلي أو خارجي.
١-٨- المخازن: إجراءات الأمن المتخذة لإصدار وتلقي ومراقبة مخزون المواد؛ أسماء الحائزين الرئيسيين المأذون لهم؛ الترتيبات المتخذة لأغراض الرصد والحراسة	N, R	حسّاسة	من المحتمل أن تفيد خصوما يخططون لارتكاب أفعال ضارة.
١-٩- خرائط عامة تُبيّن موضع مرفق وحدوده ولكن دون تقديم تفاصيل عن محتوياته	N, R	غير حسّاسة	تُبيّن تطبيقات رسم الخرائط المتاحة مجانا على شبكة الإنترنت هذه المعلومات بوضوح.
١-١٠- المسائل الأخرى المتصلة بالحماية المادية، مثل أماكن التواجد، والضبط، والموظفين والمعدات في محطة الإنذار المركزية؛ ومكان تواجد محطة الإنذار الثانوية؛ ونوع حاجز المنطقة الداخلية	N, R	حسّاسة	من شأن أي تفاصيل من هذه الطابع أن تفيد إلى حد كبير أي خصوم يرغبون في التغلّب على نظم الأمن في المرافق النووية.
٢- معلومات متصلة بكمية وشكل المواد			
٢-١- معلومات عن كمية المواد النووية ونوعها وشكلها، بما في ذلك مصادرها، المتسلمة منها أو المحتفظ بها في أماكن محددة من جميع فئات المواقع ومحطات القوى النووية، بما في ذلك الأماكن الدقيقة التي يتم فيها الاحتفاظ بالوقود المستهلك	N	حسّاسة	معلومات من هذا النوع يمكن أن تُفيد خصوما في اختيار الأهداف خلال عمليات التخطيط للهجوم.

الجدول ثانياً-١- مخطط تصنيف أمني افتراضي للمعلومات الحسّاسة المتعلقة بالأمن النووي (تابع)

الصنف	المجال	الحساسيّة	الأساس المنطقي للتأمين
٢-٢- الإنتاجية — القدرة الإسمية، القدرة الفعلية والبيانات التاريخية عن إنتاجية مرفق خاضع لضمانات الوكالة	N	غير حسّاسة	غالبًا ما تكون معلومات عالية المستوى من هذا القبيل، خاصة تلك المتعلّقة بمحطات القوى النووية منشورة في المجال العام.
٢-٣- الأرصدة، الوطنية منها أو المحلية، من الموادّ المشعّة الأخرى (بما يشمل المواد المهملة)، بما في ذلك كميتها ونوعها وشكلها ومكان تواجدها الدقيق	R	حسّاسة	معلومات من هذا النوع يمكن أن تُفيد خصوما في اختيار الأهداف خلال عمليات التخطيط للهجوم بغية سرقة موادّ مشعّة. وينبغي النظر في أي من المعلومات تكون متاحة بالفعل للجمهور فيما يتعلّق بهذه الأرصدة. ولا يجوز اعتبار جميع هذه المعلومات حساسة. وستساعد عمليات النهج الواعية بالمخاطر على تحديد ما إذا كان ينبغي تصنيف أمر ما حساسا أم لا.
٣- المواد قيد النقل (بما في ذلك عمليات النقل ضمن موقع ما)			
٣-١- معلومات عن تحركات المواد النووية من الصنف الأول والثاني والثالث	N	حسّاسة	هذه المعلومات يمكن أن تساعد على اختيار الأهداف خلال التخطيط لارتكاب أفعال ضارة تنطوي على مواد نووية قيد النقل.
٣-٢- المركبات عالية الأمن (HSVs)			
ألف- وصول مرئي إلى داخل المركبة ومقصورة الشحن	N	حسّاسة	
باء- سمات الأمن المادي لتصميم المركبة وتشييدها	N	حسّاسة	

الجدول ثانياً-١- مخطط تصنيف أمني افتراضي للمعلومات الحسّاسة المتعلقة بالأمن النووي (تابع)

الصنف		المجال	الحساسيّة	الأساس المنطقي للتأمين
	جيم- تصميم ووظيفة أجهزة الإنذار، وأجهزة شل حركة، والتصاميم الرئيسية للأقفال الخاصة	N	حسّاسة	المركبات العالية الأمن هي مركبات مصممة خصيصا لنقل المواد النووية على نحو مأمون. وتقوم المركبات العالية الأمن بحمل المواد النووية. ويمكن لأي معلومات ضمن الأنواع المدرجة في هذا القسم أن تكون مفيدة لخصم يخطط لمحاولة سرقة أو تخريب مواد نووية قيد النقل.
	دال- مفاتيح مقصورات الحمولة، ومفاتيح الغيار وإعدادات الأقفال التوافقية، حيثما تستخدم	N	حسّاسة	
	هاء- نظام تعقب المركبات إذا كان مثبتا في المركبة العالية الأمن؛ أداء النظام واتصالاته	N	حسّاسة	
٣-٣-	حاويات العبور الخاصة بالمواد النووية			
	ألف- مستوى مقاومة حاويات العبور للهجوم بواسطة وسائل مختلفة	N	حسّاسة	معلومات مفيدة لخصم يخطط لهجوم تخريبي بهدف إطلاق مواد نووية أو يخطط لسرقة مواد نووية خلال النقل.
	باء- المواصفات وبيانات التصميم الخاصّة بالحاويات	N	غير حسّاسة	غالبا ما تكون المعلومات عن تصميم حاويات من هذا القبيل دون تحديد تفاصيل التشييد متاحة على شبكة الإنترنت.
	جيم- معلومات عن تصميم حاويات معيّنة (حاويات محمية على نحو خاصّ)	N	حسّاسة	معلومات مفيدة لخصم يخطط لهجوم تخريبي بهدف إطلاق مواد نووية أو يخطط لسرقة مواد نووية خلال النقل.
٣-٤-	طرود النقل: معلومات عن تصميم طرود النقل	N	حسّاسة	معلومات مفيدة لخصم يخطط لهجوم تخريبي بهدف إطلاق مواد نووية أو يخطط لسرقة مواد نووية خلال النقل.

الجدول ثانياً-١- مخطط تصنيف أمني افتراضي للمعلومات الحسّاسة المتعلقة بالأمن النووي (تابع)

الصنف	المجال	الحساسيّة	الأساس المنطقي للتأمين
٣-٥- معلومات عن تحركات الموادّ المشعّة الأخرى	R	حسّاسة	معلومات من هذا النوع، خاصة إذا ما تعلّق الأمر بنقل مصادر إشعاعية قويّة، يمكن أن تكون مفيدة في التخطيط لسرقة.
٤- نُظَم تكنولوجيا المعلومات والنظم الحاسوبية المهمة بالنسبة إلى الأمان والأمن			
٤-١- تفاصيل نُظَم تكنولوجيا المعلومات التي تقوم بخزن ومعالجة المعلومات الحساسة، بما في ذلك النظم المستخدمة لأغراض الأمن، وبنى النظم، وتفاصيل التدابير المتخذة لأمن الحواسيب، وأماكن تواجد الوسائط الاحتياطية	N, R	حسّاسة	معلومات مفيدة لخصم يخطط لارتكاب فعل ضار في مرفق.
٤-٢- تفاصيل مراقبة الوصول، ونظم كشف الاقتحام، ونظم رصد أجهزة الإنذار، ونظم المراقبة وغيرها من وظائف وأجهزة الأمن؛ ومعلومات عن أماكن تواجد المعدات الاحتياطية والبرامج الحاسوبية الاحتياطية	N, R	حسّاسة	معلومات مفيدة لخصم يخطط لارتكاب فعل ضار في مرفق.
٤-٣- تفاصيل نُظَم تكنولوجيا معلومات أو نظم حاسوبية متصلة بالأمان وتكتسي أهمية بالنسبة إليه، بما يشمل أماكن التواجد، والوظائف، ومسارات الارتقاء، والإمداد بالطاقة والاحتياط	N, R	حسّاسة	لدى هذه النظم وظائف مراقبة ورصد تشغيلي. والنجاح في الإخلال بهذه النظم يمكن أن يُمَكِّنَ خصما، على الأقل، من تعطيل تشغيل مرفق، ويُمكن أن يؤدي هذا الإخلال في أسوأ الحالات إلى انبعاث مواد مشعة.
٥- قوات الحراسة وقوات التصدّي			
٥-١- قوات الحراسة في مرفق			
ألف- التأسيس العام للقوات وقدراتها الحالية	N	غير حسّاسة	الإشهار بوجود قوات يمكن أن يطمئن الجمهور كما أنه من المحتمل أن يكون بمثابة رادع.

الجدول ثانياً-١- مخطط تصنيف أمني افتراضي للمعلومات الحسّاسة المتعلقة بالأمن النووي (تابع)

الصنف		المجال	الحساسيّة	الأساس المنطقي للتأمين
باء-	التأسيس والقدرات الحالية في مواقع معينة	N	حسّاسة	معلومات من هذا الطابع يُمكن أن تُفيد أي خصم في التخطيط للتوغل في موقع نووي لأغراض التخريب أو السرقة، ويمكن أن تقوّض القدرة على التصدي الفعال لهجوم ما.
جيم-	أرقام بشأن أي مناوبة داخل موقع ما	N	حسّاسة	
دال-	الأسلحة وغيرها من المعدات الخاصة الأخرى المتاحة لقوات الحراسة وعدد مستخدمي الأسلحة النارية المُتَدرّبين من بين قوات حراسة فرادى المواقع	N	حسّاسة	
هاء-	مكان تواجد قوات التصدّي وقدراتها وأسلحتها ومركبات التصدي الخاص التابعة لها، وتواقيتها، في موقع ما	N	حسّاسة	ينبغي لأي معلومات، يمكن أن تساعد خصما على التقييم الاستباقي لحجم التصدي والقدرات المتاحة لوحدة عمليات تكتيكية، أن تكون مؤمنة ضد الكشف.
واو-	خطط الانتشار	N	حسّاسة	
٥-٢-	مرافقة تحركات المواد النووية			
ألف-	انتشار المرافقين وقدراتهم	N	حسّاسة	
باء-	الترددات اللاسلكية المستخدمة للتمكين من الاتصال بإحدى قوى التصدّي أو قوات الشرطة المحلية	N	حسّاسة	معلومات يمكن أن تُفيد خصما يخطط للهجوم على قافلة.

الجدول ثانياً-١- مخطط تصنيف أمني افتراضي للمعلومات الحسّاسة المتعلقة بالأمن النووي (تابع)

الصنف	المجال	الحساسيّة	الأساس المنطقي للتأمين
٦- حصر المواد النووية			
٦-١- الوصف			
ألف- بيانات متعلقة بالمبادئ العامة لحصر المواد	N	غير حسّاسة	المبادئ العامة من هذا النوع موجودة في المجال العام.
باء- استبيان المعلومات التصميمية ووصفه، وأماكن تواجد قياس المواد النووية (MBAs) ونقاط القياس الأساسية (KMPs).	N	حسّاسة	معلومات مفصلة من هذا القبيل بشأن مكان تواجد مواد نووية أو كمياتها يمكن أن تكون مفيدة لخصم يخطط لارتكاب فعل ضار.
جيم- الشكل المادي والكيميائي لقياس المواد في نقطة قياس أساسية	N	حسّاسة	
٦-٢- بيانات القياسات والأجهزة			
ألف- دقة وصحة التقنيات المختبرية المعيارية	N	غير حسّاسة	غالبًا ما تكون هذه المعلومات منشورة في المجال العام.
باء- بيانات تكشف عن حساسية القياس أو حدود أجهزة الإنذار فيما يتعلّق بمواد غير محصورة داخل محطة معيّنة	N	حسّاسة	بيانات الدقة والصحة المتصلة بقياسات فعلية أو نمطية في المواقع، سواء كانت مجمّعة أو مصنّفة، يمكن أن تكون مفيدة لخصم يخطط لسرقة مواد ما.
٦-٣- تدفّق المواد النووية ورصيد البيانات المخزنة في نُظَم تكنولوجيا المعلومات، أو في شكل نسخ ورقية، أو على أي شكل من أشكال وسائط التخزين	N	حسّاسة	معلومات يمكن أن تكشف تفاصيل دقيقة عن مكان تواجد مواد نووية وعن تحركاتها.
٦-٤- المواد غير المحصورة			

الجدول ثانياً-١- مخطط تصنيف أمني افتراضي للمعلومات الحسّاسة المتعلقة بالأمن النووي (تابع)

الصنف		المجال	الحساسيّة	الأساس المنطقي للتأمين
ألف-	الأرقام السنوية للمواد غير المحصورة بالنسبة إلى موقع ما التي لا تكشف منطقة قياس المواد النووية المعنية	N	غير حسّاسة	في العديد من الدول، تنشر الأرقام السنوية المجمّعة للمواد غير المحصورة، أو يمكن نشرها، في المجال العام.
باء-	مواد غير محصورة في مناطق قياس المواد النووية أو نقاط القياس الأساسية	N	حسّاسة	
جيم-	تفاصيل تحقيقات بشأن مواد غير محصورة معيّنة إلا إذا تمت الموافقة رسميا على نشرها	N	حسّاسة	
دال-	حد الخطأ بالنسبة إلى المواد غير المحصورة أو غيرها من الإشارات المحددة إلى انعدام اليقين بشأن أرقام المواد غير المحصورة	N	حسّاسة[أ]	ومع ذلك، فإنّ أرقاما مفصلة لمواد غير محصورة أو نتائج مفصلة لتحقيقات ما قد تكون مفيدة لخصم في استهداف مرفق محدد وينبغي بالتالي اعتبارها معلومات حساسة.
٧- طلبات متعلقة بعمليات منح التراخيص والأذون				
٧-١-	طلبات متعلقة بعمليات منح التراخيص والأذون لا تتضمّن معلومات مفصلة عن تدابير الأمن المتخذة فيما يتعلق بمواد ما؛ وعن نوع هذه المواد وشكلها وكميتها	N, R	غير حسّاسة	محتوى مطالب من هذا القبيل سيختلف تبعا للإطار القانوني والرقابي وللاستخدام النهائي المحدد. وإذا تضمّنت هذه المطالب معلومات حساسة من المحتمل أن تكون مفيدة لخصم ما، ينبغي أن تُعامل هذه المطالب أيضا على أنها معلومات حساسة.

(أ) في بعض الدول، لا يعتبر حد الخطأ بالنسبة إلى المواد غير المحصورة من المعلومات الحساسة.

الجدول ثانياً-١- مخطط تصنيف أمني افتراضي للمعلومات الحسّاسة المتعلقة بالأمن النووي (تابع)

الصنف	المجال	الحساسيّة	الأساس المنطقي للتأمين
٧-٢- طلبات متعلقة بعمليات منح التراخيص والأذون تتضمّن، على سبيل المثال، معلومات مفصلة عن تدابير الأمن المتخذة فيما يتعلق بمواد ما؛ وعن نوع هذه المواد وشكلها وكميتها	N, R	حسّاسة	محتوى مطالب من هذا القبيل سيختلف تبعا للإطار القانوني والرقابي وللاستخدام النهائي المحدد. وإذا تضمّنت هذه المطالب معلومات حساسة من المحتمل أن تكون مفيدة لخصم ما، ينبغي أن تُعامل هذه المطالب أيضاً على أنها معلومات حساسة.
٨- حالات الأمان، والوثائق المتعلقة بشؤون الهندسة وغيرها من المعلومات المتعلّقة بالأمن أو البيئة			
٨-١- حالات الأمان من جميع الأصناف			في حين أن معظم المعلومات المتعلقة بحالات الأمان يجوز إطلاع للجمهور بشأنها لأغراض الشفافية، يجوز أيضا اعتبار بعض هذه المعلومات حساسة فيما يتعلّق بالأمن النووي.
ألف- تفاصيل الأخطار المحتملة أو غيرها من المعلومات التي يمكن أن تستخدم كبديل لتقييم أثر إنطلاق أو تفاصيل عن آثار انطلاقات	N, R	حسّاسة	
باء- تفاصيل مكامن قوة وضعف العمليات والهياكل ونظم الحماية المصممة لاحتواء المواد النووية أو الموادّ المشعّة الأخرى، أو مراقبتها أو تأمينها	N, R	حسّاسة	نوع المعلومات المفصلة التي تتضمنها حالات الأمان قد تكون مفيدة لخصم في اختيار الأهداف والتخطيط لعملية ما.
جيم- تفاصيل الوصول إلى عملية الإنتاج، فيما يتعلق بمراقبة الوصول المادي وإزالة المواد من العملية لأغراض المراقبة والرصد	N, R	حسّاسة	

الجدول ثانياً-١- مخطط تصنيف أمني افتراضي للمعلومات الحسّاسة المتعلقة بالأمن النووي (تابع)

الصنف	المجال	الحساسيّة	الأساس المنطقي للتأمين
٩- خطط وتمارين الطوارئ والتصدي			
٩-١- الطوارئ والتصدي			
ألف- وجود خطة للطوارئ والتصدي	N, R	غير حسّاسة	الإشهار بوجود خطط يمكن أن يطمئن الجمهور كما أنه من المحتمل أن يكون بمثابة رادع.
باء- محتويات مفصّلة لخطة للطوارئ والتصدي	N, R	حسّاسة	بعض تفاصيل الخطة يمكن أن تُبيِّنَ القدرات والحدود والأوقات التي يستغرقها التصدي، وبالتالي، يمكن أن تُفيد خصما في التخطيط لهجوم متعمّد.
٩-٢- خطط الطوارئ الأمنية، بما يشمل المعلومات المفصلة	N, R	حسّاسة	تتضمنُ وثائق من هذا القبيل معلومات عن تدابير الأمن القائمة، وقدرات فرق قوات الشرطة أو قوات الحراسة، والتصدي المرجّح لحادث أمني ما.
٩-٣- التمارين			
ألف- أن يُقرّر إجراء تمرين ما أو إذا ما تمّ إجراؤه	N, R	غير حسّاسة	الإشهار بوجود تمارين يمكن أن يطمئن الجمهور، شريطة ألاّ يساعد مستوى ما يتمّ تقديمه من تفاصيل، مثل تاريخ/وقت/مكان إجراء تمرين مقبل، خصما ما.
باء- تفاصيل التمارين المتعلقة بالأمن في موقع ما، بما في ذلك السيناريو، وأي من جوانب خطة الأمن يجري اختبارها، وما إذا كان سيتم إشراك إحدى قوى التصدّي، ونتائج التمارين	N, R	حسّاسة	إمداد الخصوم بمعلومات عن طابع قوى التصدّي وحجمها وقدراتها وتوقيت ردّها، وعن تفاصيل بشأن قوى التصدّي المسلّحة وطابع الأساليب التكتيكية المستخدمة وخطة الإشارة.

الجدول ثانياً-١- مخطط تصنيف أمني افتراضي للمعلومات الحسّاسة المتعلقة بالأمن النووي (تابع)

الصنف	المجال	الحساسيّة	الأساس المنطقي للتأمين
جيم- تفاصيل التمارين المتعلقة بالأمان	N, R	غير حسّاسة	غالبا ما يتم إجراء التمارين المتعلقة بالأمان بصورة منفتحة وشفَّافة. وعادة ما يتم اعتبارها غير-حساسة طالما أنها لا تكشف عن معلومات مفصلة عن تدابير الأمن.
١٠- المعلومات الشخصية			
١٠-١- المعلومات الشخصية			
ألف- معلومات متأتية على إثر عمليات تحقق من الجدارة بالثقة	N, R	حسّاسة	معلومات من هذا الطابع يمكن أن يتم استخدامها لأغراض التهديد أو الابتزاز. ومعظم لوائح الخصوصية الوطنية ستنصّ على حماية هذا النوع من المعلومات.
باء- معلومات واردة في ملفات العاملين	N, R	حسّاسة	
١١- رصيد النفايات المشعّة			
١١-١- معلومات عن النفايات المشعّة			
ألف- معلومات عامة عن الأرصدة لا تتضمن أي معلومات يمكن استغلالها، من قبيل موقع معيّن يتم فيه تخزين نفايات، أو الكميات مجمّعة من النفايات التي يكون مكان تواجدها غير معلوم	N	غير حسّاسة	عمومًا، تكون هذه المعلومات منشورة في المجال العام وهي لا تُمد الخصوم بوصف لخصوصيات الاستخدام.
باء- معلومات يمكن أن تستخدم لارتكاب فعل ضار أو تُمكّن من تحديد مبنى معيّن في مرفق ما والمواد التي يتم الاحتفاظ بها فيه	N	حسّاسة	تُقدّم هذه المعلومات إلى خصم يُخطط للقيام بعمل تخريبي معلومات استهدافية.

الجدول ثانياً-١- مخطط تصنيف أمني افتراضي للمعلومات الحسّاسة المتعلقة بالأمن النووي (تابع)

الصنف	المجال	الحساسيّة	الأساس المنطقي للتأمين
١٢- الإخراج من الخدمة			
١٢-١- خطط إخراج المحطات من الخدمة	N, R	غير حسّاسة	غالبا ما يتم الإعلان للجمهور عن خطط إخراج المرافق من الخدمة.
١٢-٢- النفايات الناتجة عن الإخراج من الخدمة[ب]			
ألف- أن يُقرّر تشييد مخزن ما ومكان تشييده	N, R	غير حسّاسة	غالبا ما تكون هذه المعلومات منشورة في المجال العام.
باء- تفاصيل التشييد وتدابير الأمن المتخذة وكمية أو نوع المواد التي سيتم خزنها في المباني الجديدة لأغراض معالجة وخزن النفايات والمواد الملوثة المتأتية من أنشطة المعالجة خلال عملية الإخراج من الخدمة	N, R	حسّاسة	يمكن أن تُقدّم هذه المعلومات إلى خصم يُخطط لهجومات تخريبية معلومات استهدافية مفيدة.
١٣- معلومات عن تقييمات التهديدات والإنذار الأمني			
١٣-١- معلومات عن تقييمات التهديدات صادرة عن الدولة أو سلطات الأمن الوطنية أو غيرها من السلطات المختصّة	N, R	حسّاسة	عادة ما تستخلص من المواد المتعلقة بالأمن الوطني، مثل المعلومات الاستخبارية الوطنية.
١٣-٢- تفاصيل التهديدات المحتاط لها في التصميم	N	حسّاسة	عادة ما تستخلص من المواد المتعلقة بالأمن الوطني، مثل المعلومات الاستخبارية الوطنية.

(ب) يشير هذا الأمر أساساً إلى المواد الملوثة المتأتية من المرفق، بدلا من النفايات المشعّة المتأتية من العمليات التي يتم إجراؤها أثناء التشغيل العادي للمرفق.

الجدول ثانياً-١- مخطط تصنيف أمني افتراضي للمعلومات الحسّاسة المتعلقة بالأمن النووي (تابع)

الصنف	المجال	الحساسيّة	الأساس المنطقي للتأمين
١٣-٣- تفاصيل دراسات تحديد المجالات الحيوية	N	حسّاسة	يمكن أن تُفيد خصما في تحديد الأهداف والقيام بهجوم ما.
١٣-٤- أسباب أي حالة إنذار أمني قائمة وأسباب أي تغييرات تطرأ عليها	N, R	حسّاسة	عادة ما تستخلص من المواد المتعلقة بالأمن الوطني، مثل المعلومات الاستخبارية الوطنية.
١٤- التكنولوجيا النووية			
١٤-١- معلومات تقنية مفصّلة عن إنتاج المواد النووية أو معالجتها (مثل معالجة اليورانيوم المثرى وإعادة معالجته)	N	حسّاسة	معلومات من هذا النوع يمكن أن تكون مفيدة لخصم ما.
١٤-٢- تصاميم أو تكنولوجيات جديدة تم التقدم بمطالب بشأنها لأغراض الترخيص (مثل تكنولوجيات المفاعلات المتقدمة، وما إلى ذلك)	N	حسّاسة	على الرغم من أنّ تفاصيل هذه التكنولوجيات قد تكون متاحة للجمهور، من الممكن أن تُفيد بعض التفاصيل المتعلقة بالتصميم أو التكنولوجيا الخُصومَ لأغراض التخطيط. ويجوز استعراض هذه المعلومات لتحديد أي منها ينبغي اعتبارها معلومات حساسة.
١٤-٣- معلومات مفصلة من شأنها أن تساعد في تفكيك أجهزة بما يتيح الوصول إلى المصادر، أو أن تساعد بطرق أخرى في التغلّب على تدابير الأمن	R	حسّاسة	هذه المعلومات يمكن أن تُفيد خصما يحاول إزالة مواد مشعة.
١٤-٤- دراسات ثغرات التصاميم التكنولوجية	N, R	حسّاسة	على الرغم من أن الدراسات الآكاديمية قد تكون متاحة للجمهور فإنه ينبغي تأمين، أي معلومات مفصّلة تكشف عن ثغرات التي يمكن استغلالها من قبل خصم ما، ضدّ الكشف دون إذن.

الجدول ثانياً-١- مخطط تصنيف أمني افتراضي للمعلومات الحسّاسة المتعلقة بالأمن النووي (تابع)

الصنف	المجال	الحساسيّة	الأساس المنطقي للتأمين
١٥- المعلومات التاريخية			
١٥-١- معلومات تاريخية ذات صلة بالحالة الراهنة، لا تزال حساسة، سواء كانت مصنّفة أم لا	N, R	حسّاسة	معلومات من هذا الطابع، على الرغم من قِدَمها، قد تظل مفيدة للخصوم.

ملحوظة: HSV — مركبة عالية الأمن؛ KMP — نقطة قياس أساسية؛ MBA — منطقة لقياس المواد النووية؛ MUF — مواد غير محصورة؛ N — المواد نووية والمرافق نووية؛ R — الموادّ المشعّة الأخرى والمرافق ذات الصلة.

المرفق الثالث

عينة من برنامج التوعية بشأن الأمن

ثالثاً-١- يقدّم المرفق الثالث مثالا عن إطار ومحتوى لوضع برنامج توعية بشأن الأمن. وعند اتخاذ قرار بشأن محتوى برنامج توعية بشأن أمن المعلومات، ينبغي لمدير الأمن أن ينظر في المواضيع والأساليب المهمة تحديدا التي تم إبرازها في هذا المنشور وتكييف البرنامج وفقًا لذلك.

التدريب في مجال الأمن

ثالثاً-٢- يمكن تقسيم التدريب بصفة عامة إلى أربعة أنواع:

(أ) تدريب للتوعية يَزيدُ من مستوى الوعي بشأن التهديدات والثغرات والاعتراف بالحاجة إلى حماية البيانات والمعلومات ووسائل معالجتها (توعية بشأن أمن الحواسيب والمعلومات).

(ب) تدريب مواضيعي يشمل تنظيم دورات تدريبية لفائدة جميع الموظفين بشأن الجوانب المحددة للأمن (التعامل مع المواد المصنّفة والإجراءات المتعلّقة بالحادثات المتصلة بأمن المعلومات).

(ج) تدريب مهني يكون عادة في شكل تدريب تقني مفصّل يقدم للموظفين المناطة بعهدتهم مسؤوليات خاصّة، من بينهم مديرو النظم ومطوِّرو البرامج الحاسوبية، ومديرو الشبكات، والحرّاس الأمنيون، ومصنفو الوثائق ورافعو التصنيف عنها.

(د) وتدريب متخصص في مجال الأمن يكون مركّزا وعلى مستوى الخبراء، عادة ما يقدّم على مستوى الإدارة، في مجالات، منها، إدارة المخاطر والوقاية من الحادثات والتصدّي لها.

ثالثاً-٣- يُمكن أن يتضمَّن البرنامج محتوى لإذكاء الوعي بشأن المواضيع التالية:

(أ) لمحة عامة عن البنية الأساسية للأمن الوطني.

(ب) جوانب من أمن المعلومات ولماذا هي مهمّة بالنسبة إلى الأمن النووي.

(ج) النظام الوطني للتصنيف.

(د) مبادئ الأمن، مثل "الحاجة إلى المعرفة" و"الحاجة إلى الحيازة".

(هـ) التهديدات الراهنة للأمن الناجمة عن الأفعال المتعمّدة من قبل:

'١' دوائر الاستخبارات العدائية فيما يتعلّق بالتجسّس ونقل التكنولوجيا؛

'٢' المنظمات التخريبية؛

'٣' أفراد أو جماعات أخرى مثل وسطاء المعلومات والصحفيين الاستقصائيين الساعين إلى الوصول دون إذن إلى المعلومات الحساسة أو إلى المواقع والمرافق النووية؛

'٤' والمصادر الداخلية.

(و) التهديد المتأتي من المنظمات الخصيمة ومن الأعمال التخريبية، مع مراعاة التهديد العالمي المعاصر من قبل أيّ فصائل متطرفة.

(ز) المخاطر والعواقب المترتبة عن فقدان داخلي أو تسريبات لمعلومات حساسة، ربما من خلال سلوك غير مقصود أو للتسبب في إحراج، إلى جانب خيانة متعمّدة بسبب دوافع سياسية أو لمساعدة الإرهاب.

(ح) سلوك أو أنشطة من المرجّح أن تساعد خصوما محتملين أو أن تزيد من خطر الإخلالات، بما في ذلك:

'١' السلوك المُعَرِّضُ للخطر من قبيل المواقف العرضيّة إزاء الأمن والثرثرة؛

'٢' والسلوك غير المقصود الذي يمكن أن يجتذب اهتمام الوكالات المعادية وما ينبغي اتخاذه من الاحتياطات اللازمة تجاه ما يضطلع به من أنشطة يومية بما في ذلك، على سبيل المثال، النُهج الاجتماعية، والسفر، والمراسلات، والمعارف الشخصية.

(ط) المعلومات عن الحادثات الأمنية المواضيعية أو الأنواع الجديدة من النهج المستخدمة من قبل الوكالات المعادية، والتي ينبغي تعميمها بسرعة.

(ي) التأكيد على الإبلاغ الفوري عن جميع الظروف المشبوهة، وعن مكامن الضعف التي تتم ملاحظتها في إجراءات الأمن أو السلوك المُعَرِّض للخطر الذي يظهر لدى الزملاء — ينبغي الإطلاع على نطاق واسع بشأن وسائل القيام بذلك في كنف السريّة*.

(ك) أثر القوانين واللوائح الوطنية وأهميتها بالنسبة إلى الأفراد، على سبيل المثال، القوانين التي تحكم السرية، ومكافحة الإرهاب، والأمن، وحماية البيانات، وحرية الاطِّلاع على المعلومات، والجزاءات والعقوبات المسلطة على كل من ينتهكها.

(ل) توضيح مستويات رفع الرقابة الأمنية، وكيفية الاضطلاع بعمليات التحقق من الجدارة بالثقة، ولماذا هي ضرورية في دوائر الصناعة النووية والإشعاعية؛ وأي من مستويات الوصول تخصّ مستويات معيّنة من رفع الرقابة والجدارة بالثقة — وبالإضافة إلى ذلك، كيف يتصل كل هذا بتهديدات الأمن المذكورة أعلاه.

(م) انقطاع الخدمة (مثل منع منظمة ما من الوصول إلى المعلومات عند الحاجة إليها، بما يشمل أفعالا من قبيل السرقة) أو التدمير — خرق للتوافر.

(ن) تعديل المعلومات أو التدخل فيها دون إذن — خرق للسلامة.

(س) والكشف دون إذن — خرق للسريّة*.

ثالثاً-٤- يُمكن أن يتضمَّن البرنامج محتويات لتدريب المشاركين بشأن المواضيع التالية:

(أ) أمن المعلومات فيما يتعلّق بالمواد النووية والموادّ المشعّة الأخرى والمرافق الأخرى ذات الصلة.

(ب) الممارسات الجيدة والإجراءات الجيدة في مجال الأمن بما يشمل:

'١' الاستخدام الصحيح لوسوم التصنيف؛

'٢' الحماية المادية وأمن العاملين وأمن المعلومات (مثل الوثائق والاتصالات والحواسيب)؛

'٣' والأمثلة العملية على تطبيق القواعد والإجراءات المتعلّقة بالأمن خلال المهام التي يشارك فيها العاملون، أو سيشاركون فيها؛

'٤' والإجراءات التي يتعيّن اتخاذها في حال الاشتباه بحدوث خرق للأمن أو اكتشافه.

أساليب إضافية لتعزيز الأمن

ثالثاً-٥- بالإضافة إلى برنامج التدريب الأساسي، هنالك العديد من الأساليب الأخرى يمكن بواسطتها إطلاع العاملين والمقاولين بشأن رسائل التوعية بشأن الأمن وهي:

(أ) الرسائل الإخبارية الأمنية التي تنشرها بانتظام سلطات الأمن الوطنية. ويمكن أن تتضمن هذه الرسائل قضايا ذات أهمية مواضيعية ومشورة بشأن مجموعة من المسائل الأمنية.

(ب) الملصقات الحائطية لتذكير الأفراد بتهديدات الأمن والضوابط الأمنية الرئيسية الضرورية لمواجهتها. ويميل تأثير هذه الملصقات الحائطية إلى أن يكون مؤقتا، لذا، لا ينبغي فقط لهذه الملصقات الحائطية أن تكون معروضة على نحو بارز فحسب، بل ينبغي أيضا تغييرها باستمرار.

(ج) الملصقات لتذكير العاملين بمسؤولياتهم الشخصية في الحفاظ على الأمن عند استخدام مفردات محددة من المعدات.

(د) ملاحظات التذكير بالأمن خلال مرحلة تشغيل (إقلاع) نظام حاسوبي التي ينبغي للمستخدم أن يعترف بإطّلاعه عليها قبل انتهاء النظام الحاسوبي من الإقلاع أو تسجيل الدخول (بإمكان الأنظمة تسجيل هذه الاعترافات بحيث لا يستطيع المستخدم إنكار إطّلاعه على هذه الملاحظات.)

(هـ) ملاحظات الأمن والمجلات والنشرات التي تعدّها إدارة الأمن لتذكير الموظفين ببعض قواعد الأمن، بغية مواجهة جملة من الأمور منها حالات التراخي المحتملة في هذا الشأن.

(و) إذكاء الوعي بشأن الحالات التي وقعت فيها عمليات خرق للأمن، والدروس المستفادة التي سيتعيّن استخلاصها من هذه الحالات.

(ز) تحذير الأفراد من التهديدات المحددة أو المواضيعية للأمن وتقديم الإرشادات لمواجهتها.

(ح) توفير قناة اتصال مع الأفراد بشأن المسائل الأمنية عموما.

(ط) إجراء اختبارات دورية منتظمة لمستويات المعرفة الفردية بشؤون الأمن.

(ي) كما يمكن لشبكة إنترانات منظمة ما أن تكون بمثابة أداة قيّمة لإيصال رسائل الأمن أو الترويج لها طالما أن طابع هذه المواد وحساسيتها يظلاّن ضمن مستوى التصنيف المعتمد بالنسبة إلى هذه الشبكة.

مسرد المصطلحات

الإخلال. هو الانتهاك العرضي أو المتعمد لسرية* كائن معلومات ما، أو فقدان سلامته أو فقدان توافره.

أصول المعلومات الحسّاسة. أي معدات أو مكونات تستخدم لخزن المعلومات الحساسة أو معالجتها أو مراقبتها أو إرسالها. على سبيل المثال، تشمل أصول المعلومات الحسّاسة نظم المراقبة، والشبكات، ونظم المعلومات، وأي وسائط إلكترونية أو مادية أخرى.

أمن المعلومات. الحفاظ على سريّة* المعلومات وسلامتها وتوافرها.

التوافر. الخاصيّة المتمثلة في الإتاحة والقابلية للاستخدام بناء على الطلب من قبل كيان مأذون له.

الحاجة إلى الحيازة. قاعدة لا يُسمح بمقتضاها بأن تكون للأفراد حيازة مادية لأصول المعلومات باستثناء أصول المعلومات التي تكون ضرورية لتمكينهم من الاضطلاع بعملهم على نحو فعال.

الحاجة إلى المعرفة. قاعدة لا يُسمح بمقتضاها للأفراد وفي إطار العمليات وللنظم بالوصول إلاّ إلى المعلومات والقدرات والأصول التي تكون ضرورية لتمكينهم من تنفيذ وظائفهم المأذون بها.

السريّة*. الخاصية المتمثّلة في عدم إتاحة المعلومات أو كشفها للأفراد أو الكيانات أو خلال العمليات، دون إذن.

السلامة. خاصية دقة المعلومات وكمالها.

سلطة مختصّة. أي منظمة أو مؤسسة حكومية تم تعيينها من قبل دولة ما للاضطلاع بوظيفة أو أكثر من وظائف الأمن النووي.

كائن المعلومات. المعارف أو البيانات التي لها قيمة بالنسبة إلى المنظمة.

مادة مشعة أخرى. أي مادة مشعة أخرى لا تكون من المواد النووية

مادة نووية. أي مادّة انشطارية أو مصدرية على النحو المحدّد في المادة العشرين من النظام الأساسي للوكالة.

معلومات حسّاسة. هي المعلومات، أيا كان شكلها بما فيها البرامج الحاسوبية، التي يمكن أن يؤدي كشفها أو تعديلها أو تغييرها أو تدميرها دون إذن أو منع استخدامها دون إذن إلى الإخلال بالأمن النووي.

مواد مشعّة. أي مادّة محددة في القوانين أو اللوائح الوطنية أو من قبل هيئة رقابية باعتبارها خاضعة للتحكم الرقابي بسبب نشاطها الإشعاعي.

16-29386

يُعدّ أمن المعلومات الحسّاسة من المبادئ الأساسية في مجال الأمن النووي. والمعلومات الحسّاسة هي معلومات يمكن أن يؤدي كشفها دون إذن (أو تعديلها أو تغييرها أو تدميرها أو منع استخدامها دون إذن) إلى الإخلال بالأمن النووي أو المساعدة على ارتكاب فعل ضار ضد مرفق نووي أو منظمة عاملة في المجال النووي أو أثناء عمليات النقل. ويحدّد هذا الدليل التنفيذي المفاهيم الأساسية لأمن المعلومات التي قد تنطبق على الأمن النووي بغية مساعدة الدول الأعضاء والمنظمات المناطة بعهدتها مسؤوليات في مجال الأمن النووي على وضع إطار لأمن المعلومات.

الوكالة الدولية للطاقة الذرية
فيينا

ISBN 978–92–0–612316–4
ISSN 1816–9317