الهيئة العامة للصناعات العسكرية
General Authority for Military Industries

سياسة أمن وإدارة البيانات
لقطاع الصناعات العسكرية

المعتمدة بموجب قرار مجلس إدارة الهيئة العامة للصناعات
العسكرية رقم (ج/ت/٤٩)
وتاريخ ١٨ جمادى الآخرة ١٤٤٤ هـ الموافق ١١ يناير ٢٠٢٣م

المحتويات

المقدمة

تم إطلاق رؤية ٢٠٣٠م في عام ٢٠١٦ م؛ لإطلاق إمكانات القطاعات الاقتصادية وتعزيز التنمية الاقتصادية في المملكة العربية السعودية. وتتضمن هذه الرؤية هدفاً أساسياً، وهو توطين ما لا يقل عن (٥٠٪) من الإنفاق على المعدات العسكرية بحلول عام ٢٠٣٠م، وجاء القرار السامي الكريم من مجلس الوزراء بتأسيس الهيئة العامة للصناعات العسكرية؛ لتجسد بذلك طموح المملكة -رعاها الله- نحو تعزيز قدرات التصنيع العسكري الوطنية والسعي إلى توطين قطاع الصناعات العسكرية في المملكة، وجعله رافداً هاماً للاقتصاد الوطني؛ وبذلك تكون الهيئة هي الجهة المشرعة لقطاع الصناعات العسكرية في المملكة العربية السعودية، والمسؤولة عن تنظيمه وتطويره ومراقبة أدائه.

دور الهيئة محوري في دعم قطاع الصناعات العسكرية، وذلك يساهم بشكل أساسي في توليد فرص العمل للمواطنين، وتعزيز العائدات غير النفطية، ورفع مساهمته بشكل مباشر في الناتج المحلي الإجمالي، مما يعزز استقلالية المملكة وجاهزيتها العسكرية والأمنية، من خلال بناء قطاع صناعات عسكرية وأمنية محلية.

تمثل البيانات التي تنتجها منظومة قطاع الصناعات العسكرية أو تتلقاها أو تتعامل معها أصول وطنية قيمة ومصدراً اقتصادياً يساعد على الابتكار ويساهم في دعم التحولات الاقتصادية وتعزيز المقومات التنافسية ونظراً لأن طبيعة تلك البيانات التي تتولد أو تعالج أو تتداول داخل منظومة الصناعات تتسم بالسرية والخصوصية، ولضمان بيئة آمنة وموثوقة، قامت الهيئة بتطوير "سياسة أمن وإدارة البيانات لقطاع الصناعات العسكرية " وفقاً لأفضل الممارسات التنظيمية والتشغيلية التي تحدد تصنيف البيانات، وحمايتها، ومشاركتها وقيود تداولها.

الغرض من هذه السياسة هو تزويد المنشآت العاملة في قطاع الصناعات العسكرية بمبادئ توجيهية؛ لضمان التزامها بأنظمة ولوائح المملكة ذات الصلة بأمن وإدارة البيانات، وأن هذه السياسة لا تلغي أو تحل محل المتطلبات التنظيمية لأي من الأنظمة واللوائح الأخرى، بل تسعى إلى تسهيل وتعزيز القدرة على الامتثال داخل قطاع الصناعات العسكرية، وتعتبر مكملة للأنظمة واللوائح الصادرة من الجهات الأخرى ذات العلاقة.

الفصل الأول: أحكام عامة

المادة الأولى: التعريفات:

يقصد بالألفاظ الآتية -أينما وردت في هذا السياسة- المعاني المبينة أمام كل منها، ما لم يقتضِ السياق خلاف ذلك:

المصطلح	التعريف
المملكة	المملكة العربية السعودية.
الهيئة	الهيئة العامة للصناعات العسكرية.
السياسة	سياسة أمن وإدارة البيانات لقطاع الصناعات العسكرية.
قطاع الصناعات العسكرية	الموردون والمقاولون الرئيسيون والمقاولون من الباطن للصناعات العسكرية.
المنشأة/ المنشآت	كيان يقوم بمزاولة أي من الأنشطة العسكرية التي تقوم الهيئة بالإشراف عليها أو ترخيصها.
المرخص له	الشخص ذو الصفة الاعتبارية الذي رخص له بممارسة أي من الأنشطة الخاضعة لرقابة وإشراف الهيئة.
الطرف الثالث	جهة خارجية متعاقدة مع إحدى جهات منظومة قطاع الصناعات العسكرية على تنفيذ بعض الأعمال وتكون مصرح لها بذلك وتشمل على سبيل المثال لا الحصر الموردين، المقاولين، شركاء العمل سواءً كانوا يعملون بصفة دائمة أو مؤقتة، وبصرف النظر عن مواقع عملهم.
الجهات العسكرية والأمنية	هي وزارة الدفاع ووزارة الداخلية ووزارة الحرس الوطني ورئاسة الحرس الملكي ورئاسة أمن الدولة ورئاسة الاستخبارات العامة.
الوثائق والمحفوظات	هي الأوعية التي تحتوي على معلومات تتعلق بأعمال ومصالح الدولة، سواء نتجت هذه الأوعية عن عمل من أعمال أجهزتها أو عن سواها، ما دام أن الأمر يقتضي حفظها للحاجة إليها أو لقيمتها.

البيانات	المعلومات المحفوظة رقميًا على أنها بيانات. ويشمل ذلك -على سبيل المثال لا الحصر-: البيانات الشخصية أو التقنية أو العامة. ويتم أيضًا تصنيف المستندات والتقارير المطبوعة على أنها بيانات وفق غرض هذه السياسة.
إدارة البيانات	عملية تطوير وتنفيذ الخطط والسياسات والبرامج والممارسات، والإشراف عليها؛ لتمكين الجهات من حوكمة البيانات وتعزيز قيمتها باعتبارها أحد الأصول القيّمة والثمينة.
أمن البيانات وحمايتها	هي مجموعة الأنظمة والإجراءات والتقنيات والحلول التقنية اللازمة لحماية البيانات من الوصول أو التعديل أو الحذف غير المصرح به عليها، ويتم التعاون في هذا المجال مع جهة الاختصاص وهي الهيئة الوطنية للأمن السيبراني.
الأمن المادي	التدابير الأمنية التي تم تصميمها لمنع الوصول غير المصرح به إلى المرافق والمعدات والموارد التابعة للمنشأة، وحماية الأفراد والممتلكات من التلف أو الضرر، مثل (التجسس أو السرقة، أو الهجمات الإرهابية)، وينطوي الأمن المادي على استخدام طبقات متعددة من نظم مترابطة، تشمل الدوائر التلفزيونية المغلقة (CCTV)، وحراس الأمن، والحدود الأمنية، والإقفال، وأنظمة تحكُّم الوصول، والعديد من التقنيات الأخرى.
مخالفة أمنية	الإفصاح أو الحصول على معلومات لأشخاص غير مصرح لهم الوصول إليها، أو انتهاك السياسة الأمنية السيبرانية للجهة بالإفصاح أو الحصول على بيانات حساسة أو تسريبها أو تغييرها أو تبديلها أو تخريبها أو استخدامها دون تصريح، سواء بقصد أو بغير قصد، ويشمل ذلك مفاتيح تشفير النصوص وغيرها من المعايير الأمنية السيبرانية الحرجة.
التشفير	قواعد ووسائل تخزين ونقل البيانات والمعلومات في شكل معين، وذلك من أجل إخفاء محتواها الدلالي، ومنع الاستخدام غير المصرح به والتغيير غير الملحوظ، بحيث لا يمكن لغير الأشخاص المعنيين قراءتها ومعالجتها.
الأمن السيبراني	حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزةٍ وبرمجيات، وما تقدّمه من خدمات، وما تحتويه من بيانات، من أي اختراقٍ أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع. ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك.

المادة الثانية: أهداف السياسة:

تهدف هذه السياسة إلى حماية وإدارة جميع البيانات التي تتلقاها أو تنتجها أو تتعامل معها المنشآت العاملة في قطاع الصناعات العسكرية، مهما كان مصدرها أو شكلها أو طبيعتها.

المادة الثالثة: نطاق السياسة:

تطبق أحكام هذه الوثيقة على جميع المنشآت العاملة في قطاع الصناعات العسكرية التي تقوم بمزاولة أي من الأنشطة التي تشرف عليها الهيئة أو ترخصها ولا تنطبق هذه الوثيقة على الجهات العسكرية والأمنية.

الفصل الثاني: تصنيف البيانات وقيود تداولها من ناحية سريتها

المادة الرابعة: متطلبات الجهات الحكومية ذات الاختصاص:

على المنشآت العاملة في قطاع الصناعات العسكرية الامتثال للأنظمة واللوائح والسياسات المتعلقة بحماية وإدارة وحوكمة البيانات الصادرة من الجهات الحكومية ذات العلاقة: الهيئة الوطنية للأمن السيبراني والهيئة السعودية للبيانات والذكاء الاصطناعي" مكتب إدارة البيانات الوطنية" والمركز الوطني للوثائق والمحفوظات.

المادة الخامسة: مبادئ تصنيف البيانات وقيود تداولها من ناحية سريتها:

المبدأ الأول: (الأصل في البيانات السرية)

الأصل في بيانات قطاع الصناعات العسكرية أنها "سرية للغاية" ما لم تقتضِ طبيعتها أو حساسيتها مستويات أدنى من التصنيف والحماية.

المبدأ الثاني: (الضرورة والتناسب)

يتم تصنيف البيانات من ناحية سريتها إلى مستويات وفقاً لطبيعتها، ومستوى حساسيتها، ودرجة أثرها مع الأخذ بعين الاعتبار الموازنة بين قيمتها ودرجة سريتها.

المبدأ الثالث: (التصنيف في الوقت المناسب)

يتم تصنيف البيانات من ناحية سريتها عند إنشائها أو عند استلامها من جهات أخرى ويكون التصنيف خلال فترة زمنية محددة.

المبدأ الرابع: (المستوى الأعلى من الحماية)

يتم اعتماد المستوى الأعلى من التصنيف من ناحية سريتها عندما يتضمن المحتوى مجموعة متكاملة من البيانات ذات مستويات تصنيف مختلفة.

المبدأ الخامس: (فصل المهام)

يتم الفصل بين مهام ومسؤوليات العاملين- فيما يتعلق بتصنيف البيانات من ناحية سريتها أو الوصول إليها أو الإفصاح عنها أو استخدامها أو التعديل عليها أو إتلافها بطريقة تحول دون تداخل الاختصاص.

المبدأ السادس: (الحاجة إلى المعرفة)

يتم تقييد الوصول إلى البيانات واستخدامها على أساس الاحتياج الفعلي للمعرفة، ولأقل عدد ممكن من العاملين.

المادة السادسة: مستويات تصنيف البيانات والوثائق:

١. تصنيف البيانات الرقمية:

الجدول أدناه يوضح المستويات الرئيسية لتصنيف البيانات من ناحية سريتها بما يتوافق مع مستوى الأثر، كما يوضح بعض الأمثلة الاسترشادية لكل مستوى بناء على السياسات الوطنية الصادرة من مكتب إدارة البيانات الوطنية.

مستوى التصنيف	درجة الأثر	الوصـــــف
سري للغاية	عالي	تصنـف البيـانـات على أنهـا «بيانات سرية للغاية»، إذا كان الوصول غير المصرح به إلى هذه البيانات أو الإفصاح عنها أو عن محتواها يؤدي إلى ضرر جسيم واستثنائي لا يمكن تداركه أو إصلاحه على : • المصالح الوطنية بما في ذلك الإخلال بالاتفاقيات والمعاهدات أو إلحاق الضرر بسمعة المملكة أو بالعلاقات الدبلوماسية والانتماءات السياسية أو الكفاءة التشغيلية للعمليات الأمنية أو العسكرية أو الاقتصاد الوطني أو البنية التحتية الوطنية أو الأعمال الحكومية • أداء الجهات العامة مما يلحق ضرر بالمصلحة الوطنية . • صحة الأفراد وسلامتهم على نطاق واسع وخصوصية كبار المسؤولين. • الموارد البيئية أو الطبيعية.
سري	متوسط	تصنف البيانات على أنها «بيانات سرية»، إذا كان الوصول غير المصرح به إلى هذه البيانات أو الإفصاح عنها أو عن محتواها يؤدي إلى ضرر جسيم على : • المصالح الوطنية مثل إلحاق ضرر جزئي بسمعة المملكة والعلاقات الدبلوماسية أو الكفاءة التشغيلية للعمليات الأمنية أو العسكرية أو الاقتصاد الوطني أو البنية التحتية الوطنية والأعمال الحكومية • يحدث خسارة مالية على المستوى التنظيمي تؤدي إلى إفلاس أو عجز الجهات عن أداء مهامها أو خسارة جسيمة للقدرة التنافسية أو كليهما معاً. • يتسبب في حدوث أذى جسيم أو إصابة تؤثر على حياة مجموعة من الأفراد. • تؤدي إلى ضرر على المدى الطويل للموارد البيئية أو الطبيعية • التحقيق في القضايا الكبرى المحددة نظاماً، كقضايا تمويل الإرهاب
مقيد	منخفض	تصنف البيانات على أنها «مقيدة»، إذا كان الوصول غير المصرح به إلى هذه البيانات أو الإفصاح عنها أو عن محتواها يؤدي إلى : • تأثير سلبي محدود على عمل الجهات العامة أو الأنشطة الاقتصادية في المملكة أو على عمل شخص معين . • ضرر محدود على أصول أي جهة وخسارة محدودة على وضعها المالي والتنافسي . • ضرر محدود على المدى القريب للموارد البيئية أو الطبيعية.

عام	لا يوجد	تصنف البيانات على أنها »بيانات عامة« عندما لا يترتب على الوصول غير المصرح به إلى هذه البيانات أو الإفصاح عنها أو عن محتواها أي من الاثار المذكورة أعلاه في حال عدم وجود تأثير على ما يأتي : • المصلحة الوطنية • أنشطة الجهات • مصالح الأفراد • الموارد البيئة

٢. تصنيف الوثائق والمحفوظات:

على المنشآت العاملة في القطاع تطبيق تصنيف درجات سرية الوثائق والمحفوظات لكافة تعاملاتها مع الجهات العسكرية والأمنية، وذلك على النحو التالي:

مستوى التصنيف	الوصف
وثائق ومحفوظات سرية للغاية	وهي الوثائق والمحفوظات التي تؤدي معرفة بياناتها للغير إلى الإضرار بأمن الدولة. ومن أنواع هذه الوثائق: وثائق الخطط العسكرية، وكميات الأسلحة، وأنواعها ومواقعها. ولا يجوز عادة الاطلاع على هذه الوثائق خلال مدة حظرها إلا من قبل كبار المسئولين المعنيين بمثل هذه الوثائق، أو المحاكم المعنية بالنظر في قضايا أمن الدولة وبالقدر الضروري للفصل في هذه القضايا.
وثائق ومحفوظات سرية جداً	وهي الوثائق والمحفوظات التي يؤدي إفشاء بياناتها إلى الإضرار بالمصالح العامة أو الخاصة، ومن أنواع هذه الوثائق: الوثائق المتعلقة بالأسرار الإدارية، والوثائق المتعلقة بالأسرار الصناعية، والوثائق المتعلقة بالأسرار التجارية. ولا يتم الاطلاع عادة على هذه الوثائق خلال مدة حظرها إلا من قبل المختصين.
وثائق ومحفوظات سرية	وهي الوثائق والمحفوظات التي تتعلق بمواضيع أو قضايا فردية يترتب على إفشائها أو الاطلاع عليها تأثيرات سيئة على الحياة الاجتماعية للجماعات أو الأفراد. ومن أنواع هذه الوثائق: وثائق التحقيقات والأحكام المتعلقة بقضايا الأفراد. ولا يتم الاطلاع عادة على هذه الوثائق إلا من قبل المختصين.

المادة السابعة: ضوابط تصنيف البيانات:

بناءً على مستويات تصنيف البيانات من ناحية سريتها، تقوم المنشآت العاملة في قطاع الصناعات العسكرية بما يلي:

١- تحديد وتطبيق الضوابط المناسبة لحماية البيانات وذلك لضمان التعامل معها ومعالجتها ومشاركتها والتخلص الآمن منها.

٢- في حال عدم تصنيف البيانات عند إنشائها أو عند استلامها وفقاً لمعايير التصنيف المعتمدة، تعامل هذه البيانات على أنها سرية للغاية حتى يتم تصنيفها بشكل صحيح.

ويمكن للمنشآت العاملة في قطاع الصناعات العسكرية استخدام الضوابط الموضحة أدناه عند تصنيف البيانات، والتي منها ما يلي:

- **علامة الحماية**

تطبق علامات الحماية النصية على الوثائق الورقية والإلكترونية بما في ذلك رسائل البريد الإلكتروني وفقاً لكل مستوى من مستويات التصنيف.

- **الوصول**

يسمح بالوصول إلى البيانات بناءً على مبدأ "الحد الأدنى من الامتيازات" و " الحاجة إلى المعرفة".

- **الاستخدام**

يتم تقييد استخدام البيانات المصنفة سرية للغاية - على سبيل المثال لا الحصر - على مواقع محددة سواء مادية مثل المكاتب أو افتراضية وذلك باستخدام الأجهزة أو تطبيقات خاصة.

- **التخزين**

لا تترك دون مراقبة البيانات المصنفة على أنها سرية للغاية أو سرية أو مقيدة وكذلك الأجهزة المحمولة التي تعالج أو تخزن هذه البيانات.

- **مشاركة البيانات**

تقوم الجهات بتحديد الوسائل المادية والرقمية المناسبة لتبادل البيانات بشكل آمن بما يضمن تقليل المخاطر المحتملة وتطبيقاً لأنظمة مشاركة البيانات.

- **الاحتفاظ بالبيانات**

يتم إعداد جدول زمني يحدد فترة الاحتفاظ بجميع البيانات كما يتم تحديد فترة الاحتفاظ بناءً على ما تحدده المتطلبات التجارية والتعاقدية والتنظيمية والقانونية ذات العلاقة.

- **التخلص من البيانات**
  - يتم التخلص من جميع البيانات بشكل آمن ووفقاً للجدول الزمني للاحتفاظ بالبيانات.
  - يتم التخلص من البيانات التي تم تصنيفها على أنها سرية وسرية للغاية التي يتم التحكم بها إلكترونياً باستخدام أحدث طرق التخلص من الوسائط الإلكترونية.

- يتم التخلص من جميع الوثائق الورقية باستخدام آلة تمزيق الورق (Micro-cut paper shredders).
- يتم إعداد سجل مفصل عن جميع البيانات التي تم التخلص منها.

- **الأرشفة**
  - يتم أرشفة البيانات في مواقع تخزين آمنة.
  - يتم الاحتفاظ بنسخ احتياطية من البيانات المؤرشفة.
  - تتم حماية البيانات المؤرشفة التي تم تصنيفها على أنها سرية للغاية وسرية باستخدام أحد طرق التشفير المعتمدة من قبل الهيئة الوطنية للأمن السيبراني.
  - يتم إعداد وتوثيق قائمة مفصلة تتضمن المستخدمين المصرح لهم بالوصول إلى البيانات المؤرشفة.

المادة الثامنة: التزامات المنشآت المتعلقة بتصنيف البيانات وقيود تداولها:

١. يجب على جميع المنشآت العاملة في قطاع الصناعات العسكرية تحديد جميع البيانات التي تمتلكها وفقاً لأحكام هذه السياسة.
٢. يجب على المنشآت العاملة في قطاع الصناعات العسكرية تعيين مسؤول لتصنيف البيانات يتولى مسؤولية عملية التصنيف وتحديد جميع البيانات.
٣. يجب على المنشآت العاملة في قطاع الصناعات العسكرية تكليف من يتولى مسؤولية أداء الالتزامات المسندة لها، وكذلك مسؤولية أداء الالتزامات الوظيفية المرتبطة بعملية تصنيف البيانات وشروط حمايتها.
٤. يجب على المنشآت العاملة في قطاع الصناعات العسكرية اتباع الخطوات اللازمة لعملية تقييم الأثر المحتمل الذي يترتب على الإفصاح عن البيانات أو الوصول غير المصرح به لها، أو إجراء تعديل على البيانات أو إتلافها أو كليهما.

المادة التاسعة: قيود تداول البيانات والوثائق المصنفة:

١) تستخدم عبارات محددة كقيود لتداول أو التحكم في الوصول للبيانات تتناسب مع حساسيتها ومن يمكنه الوصول لها والاطلاع عليها.
٢) يحدد قيد التداول بصياغة مرادفة لدرجة تصنيف سري وسري للغاية مثل: يفتح بيده، محدود التداول، غير قابل للتداول، نسخة ( ) من ( ).
٣) قد يتطلب الأمر السماح للسعوديين فقط بالوصول أو الاطلاع على البيانات، وفي هذه الحالة يستخدم قيد التداول "للسعوديين فقط" (SAUDI EYES ONLY).
٤) تحديد قيد التداول يقع على عاتق منشئ أو معالج البيانات (مالك البيانات).

٥) يجب أن يكون قيد التداول مناسب للغرض المستخدم لأجله.

٦) فيما يلي توضيح لقيود تداول البيانات والوثائق:

صياغة القيد	الوصف
يفتح بيده	يحدد الشخص (بوظيفته) الذي يمكنه الاطلاع على المعلومة، ويجب ألا يطلع غيره عليها مالم يتطلب الحال غير ذلك على أن تكون تحت مسؤوليته وإشرافه.
محدود التداول	يصرح بتداول البيانات في نطاق ضيق بحسب الحاجة، كأن يكون التداول داخل إدارة أو قسم أو مجموعة عمل محددة فقط.
غير قابل للتداول	لا يسمح بتداول البيانات مع الغير، ويجب أن تقف البيانات عند المصرح له بالاطلاع عليها فقط.
نسخة ( ) من ( )	يحدد العدد الكلي للنسخ المسموح بتوزيعها، على أن يكون لكل نسخة رقم تسلسل وتسلم بسند وثيقة محمية للمصرح له بالاطلاع عليها فقط.
للسعوديين فقط	عندما يتطلب الأمر عدم السماح بالاطلاع على البيانات إلا للسعوديين فقط.

الفصل الثالث: حماية البيانات

المادة العاشرة: مسؤوليات المنشآت المتعلقة بحماية البيانات:

- يجب على المنشأة إعداد وتطبيق سياسات وإجراءات بشأن حماية البيانات وفقاً لهذه السياسة وجميع الأنظمة واللوائح ذات الصلة بحماية البيانات في المملكة.
- يجب على المنشأة تطبيق الضوابط التشريعية الصادرة عن الهيئة الوطنية للأمن السيبراني وما يصدر عنها مستقبلاً من ضوابط تشريعية وتشمل مايلي :
  أ. الضوابط الأساسية للأمن السيبراني.
  ب. ضوابط الأمن السيبراني للأنظمة الحساسة.
  ت. ضوابط الأمن السيبراني للبيانات.
  ث. ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي.
  ج. ضوابط الأمن السيبراني للحوسبة السحابية.
  ح. ضوابط الأمن السيبراني للعمل عن بعد.
  خ. ضوابط الأمن السيبراني للأنظمة التشغيلية.

- يجب أن تقوم المنشأة بالتأكد أن جميع مرافقها المادية التي يتم توليد أو معالجة أو تداول البيانات المصنفة فيها تتمتع بعوامل الأمن والسلامة.
- يجب على المنشأة تحديد جميع مرافقها الداخلية التي يتم توليد أو معالجة أو تداول البيانات المصنفة فيها، ويعين لها تصنيف أمني يتناسب مع درجات تصنيف البيانات.
- يجب على المنشأة – عند الحاجة - لتطوير مخطط الأمن المادي للمرافق توزيعه إلى مناطق، تكون كل منطقة معلمة بلون يميزها بحيث يكون لكل منطقة ما يناسبها من قيود وصول بحسب تصنيفها، ويكون تصنيف المناطق على النحو الآتي:

أ. **المنطقة العامة والاستقبال (المنطقة الخضراء):** قيود محدودة وتخضع للمراقبة العامة، ويتم فيها التعامل مع المعلومات غير المصنفة.

ب. **منطقة المكاتب العامة (المنطقة الصفراء):** دخول محدود، ويتم تسجيل الدخول، ومرافقة الزوار الذين يسمح لهم بدخول هذه المنطقة، وهي تخضع للمراقبة العامة، ويتم فيها التعامل مع المعلومات المصنفة "محظور".

ج. **منطقة الدخول الآمنة (المنطقة البرتقالية):** دخول محدود جداً، ويتم تسجيل الدخول، ومرافقة الزوار الذين يتطلب العمل دخولهم إلى هذه المنطقة، وهي تخضع للمراقبة والإشراف المباشر، ويتم فيها التعامل مع المعلومات المصنفة "سري" فأقل.

د. **منطقة الدخول المقيد (المنطقة الحمراء):** دخول يخضع لقيود عالية، يقتصر الدخول للأشخاص المصرح لهم فقط، ويتم تسجيل الدخول، ويجب الحصول على تصريح دخول خاص لكل من يدخل هذه المنطقة، وهي تخضع للمراقبة والإشراف المباشر، ويتم فيها التعامل مع المعلومات المصنفة "سري للغاية".

- يجب على المنشأة التحكم في مَن له حق الدخول إلى مرافقها وفقًا للمعايير الأمنية التي تحددها الجهات المختصة، ويشمل -على سبيل المثال لا الحصر- آليات التحكم في الدخول وأنظمة الكشف والتتبع.
- يجب على المنشأة استخدام التدابير الأمنية المناسبة كالتشفير وعزل بيئة التطوير والاختبار عن بيئة التشغيل الآمن.
- يجب على المنشأة تخزين البيانات ومعالجتها داخل الحدود الجغرافية للمملكة لضمان المحافظة على السيادة الوطنية لهذه البيانات ولا يجوز معالجتها خارج المملكة إلا بعد حصول المنشأة على موافقة الهيئة.
- يجب على المنشأة توثيق سياسة وإجراءات التخلص من البيانات، وأن يكون اتلاف البيانات بطريقة آمنة تمنع فقدانها أو استخدامها أو الوصول غير المصرح لها، وتشمل البيانات التشغيلية والمؤرشفة والنسخ الاحتياطية، وذلك وفقاً لما يصدر من الهيئة الوطنية للأمن السيبراني من تعليمات.

- يجب على المنشأة تضمين أحكام سياستي الاحتفاظ والتخلص من البيانات في العقود في حال إسناد هذه المهام إلى أي طرف ثالث.
- يجب على المنشأة التحقق من هوية الأفراد قبل منحهم صلاحية الوصول إلى البيانات وفقاً لضوابط هذه السياسة، وضوابط الجهات ذات العلاقة في المملكة (الهيئة الوطنية للأمن السيبراني).
- يحظر على المنشأة مشاركة المعلومات مع أي جهة خارجية إلا بعد أخذ الموافقة الرسمية من مالك البيانات على ألا تحتوي هذه المعلومات على بيانات سرية وحساسة قد تمس بالأمن الوطني، وفقاً للأغراض المحددة، ووفقاً للأنظمة والسياسات ذات العلاقة في المملكة على أن يتم تزويد الجهة بسياسة وإجراءات الخصوصية المتبعة وتضمينها في العقود والاتفاقيات.
- يجب على المنشأة إعداد برامج توعوية لمنسوبيها لتعزيز ثقافة حماية البيانات ورفع مستوى الوعي.

المادة الحادية عشرة: الإبلاغ عن مخالفات أمن البيانات لقطاع الصناعات العسكرية:

يجب على المنشآت العاملة في قطاع الصناعات العسكرية تطبيق الأحكام التالية في حال اكتشاف مخالفات متعلقة بأمن البيانات، وهي:

أ. إبلاغ الهيئة والجهات ذات الصلة على الفور عن أي مخالفات أمنية للبيانات بمجرد اكتشافها.

ب. إعداد تقرير يتضمن جميع المعلومات ذات الصلة بالمخالفة الأمنية وتقييم الأثر الأولي لها.

ج. الاحتفاظ بسجل "للمخالفات الأمنية"، ويخضع السجل للتفتيش من الهيئة وفق الأنظمة والإجراءات.

د. للهيئة الحق في تدقيق سجلات الحوادث الخاصة بالمرخَّص لهم؛ لتقييم الامتثال لما ورد في هذه السياسة.

الفصل الرابع: مخالفة أحكام السياسة

المادة الثانية عشرة: المخالفات والجزاءات الإدارية:

للهيئة في حالة مخالفة المنشأة لأي من أحكام هذه السياسية اتخاذ الجزاءات الإدارية المناسبة حسب نوع وطبيعة وجسامة المخالفة:

١. الإنذار الإداري للمنشأة المخالفة، متضمناً تفاصيل المخالفة والإجراء الذي يجب اتخاذه من قبل المنشأة، والمهلة الممنوحة من قبل الهيئة للتصحيح.

٢. تعليق الترخيص حسب المدة التي تراها الهيئة، ولها تجديد تلك المدة عند عدم قيام المنشأة بالتصحيح.

٣. المنع من التقديم على المنافسات المستقبلية للعقود العسكرية.

٤. إلغاء الترخيص.

الفصل الخامس: أحكام ختامية

المادة الثالثة عشرة:

١. للهيئة حق تفسير ومراجعة وتحديث هذه الوثيقة عند الحاجة، والرفع بمقترح التحديث إلى مجلس الإدارة.
٢. كل ما لم يرد به نص خاص في هذه الوثيقة يطبق بشأنه تنظيم الهيئة ولوائحها وقراراتها المعتمدة.
٣. مع عدم الإخلال بالمتطلبات التنظيمية الواردة في الأنظمة واللوائح الأخرى، تعد هذه السياسية ملزمة للمنشآت وتسعى لتسهيل وتعزيز الامتثال داخل القطاع.
٤. يعمل بهذه السياسة اعتباراً من تاريخ اعتمادها ونشرها.