الهيئة العامة للصناعات العسكرية
General Authority for Military Industries

سياسة أمن البيانات لقطاع الصناعات العسكرية

المعتمدة بموجب قرار مجلس الإدارة رقم (ج/ت/٤٩) وتاريخ ١٤٤٤/٠٦/١٨هـ الموافق ٢٠٢٣/٠١/١١م

والمُعدلة بموجب قرار اللجنة التنفيذية لمجلس الإدارة رقم (ذ/٥/٣٠) وتاريخ ١٤٤٨/٠٤/٢٣هـ الموافق ٢٠٢٦/١٠/٠٤م

GAMI - Public عام

المحتويات

١. المقدمة ٣

٢. الفصل الأول: أحكام عامة ٤

٣. الفصل الثاني: حماية البيانات ٥

٤. الفصل الثالث: قيود تداول البيانات من ناحية سريتها ٨

٥. الفصل الرابع: مخالفة أحكام السياسة ٩

٦. الفصل الخامس: أحكام ختامية ١٠

المقدمة

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 البيانات لقطاع الصناعات العسكرية" وفقاً لأفضل الممارسات التنظيمية والتشغيلية التي تحدد 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 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 هذه -السياسة - المعاني المبينة أمام كل منها، ما لم يقتض السياق خلاف ذلك:

المصطلح	التعريف
المملكة	المملكة العربية السعودية.
الهيئة	الهيئة العامة للصناعات العسكرية.
السياسة	سياسة أمن البيانات لقطاع الصناعات 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 أو السجلات التي يتم إنشاؤها أو جمعها او معالجتها أو تخزينها أو نقلها أو تداولها، سواءً كانت رقمية أو مادية، مهيكلة او غير مهيكلة، والتي تتطلب الحماية من التهديدات والمخاطر السيبرانية.
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 تحكم 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 أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات من أي اختراق 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 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 السياسة على جميع المنشآت العاملة في قطاع الصناعات العسكرية التي تقوم بمزاولة أي من الأنشطة التي تشرف عليها الهيئة أو ترخصها ولا تنطبق على الجهات العسكرية والأمنية.

الفصل الثاني: حماية البيانات

المادة الرابعة: متطلبات الجهات الحكومية ذات الاختصاص:

على المنشآت العاملة في قطاع الصناعات العسكرية الامتثال للأنظمة واللوائح والسياسات المتعلقة بحماية البيانات الصادرة عن الجهات الحكومية ذات العلاقة.

المادة الخامسة: مسؤوليات المنشآت المتعلقة بحماية البيانات:

١. يجب على المنشأة إعداد وتطبيق سياسات وإجراءات بشأن حماية البيانات وفقاً لهذه السياسة وجميع الأنظمة واللوائح ذات الصلة بحماية البيانات في المملكة.

٢. يجب على المنشأة تطبيق الضوابط التشريعية الصادرة عن الهيئة الوطنية للأمن السيبراني وما يصدر عنها مستقبلاً من ضوابط تشريعية وتشمل ما يلي:

١) الضوابط الأساسية للأمن السيبراني.

٢) ضوابط الأمن السيبراني للأنظمة الحساسة.

٣) ضوابط الأمن السيبراني للبيانات.

٤) ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي.

٥) ضوابط الأمن السيبراني للحوسبة السحابية.

٦) ضوابط الأمن السيبراني للعمل عن بعد.

٧) ضوابط الأمن السيبراني للأنظمة التشغيلية.

٨) ضوابط الأمن السيبراني لجهات القطاع الخاص من غير ذوات البنى التحتية الحساسة.

كما يجب على المنشأة عند معالجة البيانات الشخصية الالتزام بنظام حماية البيانات الشخصية ولوائحه التنفيذية، وبسياسة حماية البيانات الشخصية لقطاع الصناعات العسكرية، ويقدم حكم النظام ولوائحه عند التعارض.

المادة السادسة: مسؤوليات المنشآت في حماية البيانات المتعلقة بالأمن المادي:

١. يجب أن تقوم المنشأة بالتأكد أن جميع مرافقها المادية التي يتم توليد أو معالجة أو تداول البيانات المصنفة فها تتمتع بعوامل الأمن والسلامة.

٢. يجب على المنشأة تحديد جميع مرافقها الداخلية التي يتم توليد أو معالجة أو تداول البيانات المصنفة فيها، وتعين لها تصنيف أمني يتناسب مع درجات تصنيف البيانات.

٣. 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:

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

٢) **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 "مقيد ".

٣) **منطقة الدخول الأمنة (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.

٤) **منطقة الدخول المقيد (المنطقة الحمراء):** دخول يخضع القيود 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".

٤. يجب على المنشأة التحكم في مَن له حق الدخول إلى مرافقها وفقاً للمعايير الأمنية التي تحددها الجهات المختصة، ويشمل على سبيل المثال لا الحصر آليات التحكم في الدخول وأنظمة الكشف والتتبع.

٥. يجب على المنشأة استخدام التدابير الأمنية المناسبة كالتشفير وعزل بيئة التطوير والاختبار عن بيئة التشغيل الآمن.

٦. 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.

٧. يجب على المنشأة توثيق سياسة وإجراءات التخلص من البيانات، وأن يكون إتلاف 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.

٨. يجب على المنشأة تضمين أحكام سياستي الاحتفاظ والتخلص من البيانات في العقود في حال إسناد هذه المهام إلى أي طرف ثالث.

٩. 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).

١٠. 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.

١١. يجب على المنشأة إعداد برامج توعوية لمنسوبيها لتعزيز ثقافة حماية البيانات ورفع مستوى الوعي.

الفصل الثالث: قيود تداول البيانات من ناحية سريتها

المادة السابعة: 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 الرابع: مخالفة أحكام السياسة

المادة الثامنة: 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:

١. إبلاغ الهيئة والجهات ذات الصلة على الفور عن أي مخالفات أمنية للبيانات بمجرد اكتشافها.
٢. إعداد تقرير يتضمن جميع المعلومات ذات الصلة بالمخالفة الأمنية وتقييم الأثر الأولي لها.
٣. الاحتفاظ بسجل "للمخالفات الأمنية"، ويخضع السجل للتفتيش من الهيئة وفق الأنظمة والإجراءات.
٤. للهيئة الحق في تدقيق سجلات الحوادث الخاصة بالمرخص لهم؛ لتقييم الامتثال لما ورد في هذه السياسة.

المادة التاسعة: 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 العاشرة:

١. للهيئة حق تفسير ومراجعة وتحديث هذه السياسة عند الحاجة، والرفع بمقترح التحديث إلى صاحب الصلاحية.
٢. كل ما لم يرد به نص خاص في هذه السياسة 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 نشرها.