المملكة العربية السعودية
وزارة الداخلية
الأمن العام - شؤون التدريب

مدينة تدريب الأمن العام بمنطقة القصيم

دليل سياسات سرية المعلومات

١٤٤٦هـ / ٢٠٢٤م

مدينة تدريب الأمن العام بمنطقة القصيم

دليل سياسات سرية المعلومات

مقيّد - داخلي

التاريخ: 12/11/2024
الإصدار: 1.0
المرجع: التقنية والذكاء الأصناعي

اعتماد الوثيقة

الدور	المسمى الوظيفي	الاسم	التاريخ	التوقيع
المُراجع	مدير مكتب إدارة البيانات	مقدم/ماجد بن محمد المالكي	11/12/2024	
المُراجع	مدير إدارة الأمن السيبراني	عقيد/طلال بن سويلم العتيبي	11/12/2024	
المُوافقة	مساعد مدير الأمن العام للتقنية والذكاء الاصطناعي	عقيد/محمد بن عبدالله بن جريس	1/1/2025	
المعتمِد	معالي مدير الأمن العام	فريق/محمد بن عبدالله البسامي	2/1/2025	

نسخ الوثيقة

النسخة	التاريخ	أُعد بواسطة	التوقيع
1.0	15/11/2024	ملازم أول/معاذ ناصر العدواني	
1.0	15/11/2024	ملازم اول/يوسف محمد الحربي	

جدول المراجعة

معدل المراجعة	التاريخ لأخر مراجعة	تاريخ المراجعة القادمة
مره واحدة كل سنتين	11/12/2024	11/12/2024

قائمة المحتويات

الغرض

الغرض من هذا الدليل هو ايضاح سياسات وضوابط الأمن السيبراني وسياسات البيانات التي تعنى في الحفاظ على سرية البيانات والمعلومات وحمايتها وحماية الأصول المعلوماتية والتقنية بالأمن العام المعتمدة والتي تهدف إلى الآتي:

١. مساعدة منسوبي الأمن العام على تحقيق أعلى مستويات المحافظة على سرية البيانات والمعلومات.
٢. إجراءات وضوابط حماية بيانات ومعلومات العملاء والمتعاقدين مع الأمن العام ومنع الضرر بهم.
٣. آلية الامتثال للأنظمة واللوائح المعمول بها المتعلقة بالمحافظة على سرية البيانات والمعلومات.
٤. حظر الاستخدام غير المناسب للمعلومات التي يحتفظ بها الأمن العام.
٥. ضمان حقوق ملكية البيانات والمعلومات والسجلات والملفات وغيرها والتأكد من حصر حق الوصول إليها للمخولين فقط.
٦. الارشادات الواجب اتباعها للمحافظة على سرية البيانات والمعلومات.
٧. حماية خصوصية البيانات والمعلومات الشخصية

نطاق العمل

ينطبق هذا الدليل على جميع البيانات والأصول المعلوماتية والتقنية والمعدات التي يتم تخزينها ومعالجتها ونقلها من خلال الأصول المعلوماتية والتقنية، وعلى جميع العاملين (الموظفين والمتعاقدين) في الأمن العام.

السياسات

- الأمن المادي
- أمن ووسائط التخزين
- حماية البيانات
- الاستخدام المقبول للوصول
- الأمن السيبراني المتعلق بالأطراف الخارجية
- الطابعات والماسحات الضوئية
- تصنيف البيانات
- حماية البيانات الشخصية
- مشاركة البيانات

الأمن المادي

لأهمية الأمن المادي وحماية الأصول المادية والتقنية تم اعتماد سياسة **"الأمن السيبراني المتعلق بالأمن المادي"** والغرض من هذه السياسة هي لحماية الأصول المادية والتقنية من التهديدات والمخاطر التي يمكن أن تؤثر على سلامة البيانات والأنظمة وتساعد هذه السياسة في تعزيز بيئة عمل آمنة وتحمي المعلومات الحساسة من التهديدات المختلفة، وتهدف السياسة إلى الآتي:

١. حماية الأصول المادية لتأمين الأجهزة والخوادم من الوصول الغير مصرح به.
٢. تأمين المعلومات الحساسة لضمان حماية البيانات والمعلومات الحيوية من التسرب والفقدان.
٣. حماية السجلات ومصادر المعلومات من الوصول غير المصرّح به.
٤. تنظيم الأجهزة والمعدات داخل المباني وخارجها.

أمن وسائط التخزين

لأهمية أمن وسائط التخزين تم اعتماد سياسة "أمن وسائط التخزين" والغرض من هذه السياسة هي حماية المعلومات والبيانات المخزنة من التهديدات والمخاطر وتساعد هذه السياسة في ضمان وسلامة أمان البيانات المخزنة مما يقلل من المخاطر المترتبة على الوصول غير المصرح به او فقدان البيانات، وتهدف السياسة إلى الآتي:

١- حظر استخدام أجهزة الوسائط القابلة للإزالة ما لم يكن هناك حاجة عمل تقضي باستخدامها.
٢- إعتماد وضع وتطبيق إجراءات رسمية للموافقة على استخدام الوسائط القابلة للإزالة.
٣- الإشراف على التحكم بأجهزة الوسائط ماديًا وتخزينها بشكل آمن في الأمن العام.
٤- تقييد استخدام وسائط التخزين الخارجية وتوفير سبل التعامل الآمن معها.

حماية البيانات

في ظل ضرورة حماية المعلومات والبيانات تم اعتماد سياسة **"الأمن السيبراني لحماية البيانات"** والغرض من هذه السياسة هي حماية المعلومات الحساسة وضمان سريتها وسلامتها وتساعد هذه السياسة في الحفاظ على امان البيانات وضمان الالتزام بالمعايير القانونية والتنظيمية المتعلقة بحماية المعلومات، وتهدف السياسة إلى الآتي:

١- الالتزام بالمتطلبات التشريعية والتنظيمية المتعلقة بحماية البيانات في المملكة العربية السعودية، والسياسات والإجراءات المتبعة في الأمن العام.
٢- استخدام خاصية العلامات المائية (watermark feature) لترميز الوثيقة بأكملها عند إعدادها، أو تخزينها، أو طباعتها، او عرضها على الشاشة، والتأكد من احتواء كل نسخة من الوثيقة على رقم يمكن تتبعه.
٣- تأمين خصوصية البيانات والمعلومات.
٤- جميع البيانات والمعلومات تعود ملكيتها لـلأمن العام.
٥- عدم حفظ البيانات المصنفة (سرية، سرية للغاية) في أجهزة تخزين محمولة مثل الأقراص الصلبة الخارجية أو وحدات التخزين "USB"، بغض النظر عن مستوى التشفير المستخدم في جهاز التخزين المحمول.

الاستخدام المقبول للأصول.

لتحقيق ضوابط استخدام الاصول التقنية تم اعتماد سياسة **" الامن السيبراني للاستخدام المقبول للاصول"** والغرض من هذه السياسة وضع إطار عمل واضح يحدد كيفية استخدام المواد التقنية المتاحة في الأمن العام التي تساعد في تعزيز الوعي الأمني وتقليل المخاطر المرتبطة بالاستخدام الغير مناسب للموارد وتغطي هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة بالأمن العام وتطبق على جميع العاملين في الأمن العام، وتهدف هذه السياسة إلى الآتي:

١- عدم ترك المطبوعات على الطابعة المشتركة دون رقابة.
٢- حفظ وسائط التخزين الخارجية بشكل آمن ومناسب، مثل التأكد من ضبط درجة الحرارة بدرجة ملائمة، وحفظها في مكان معزول وآمن.
٣- الالتزام بسياسة المكتب الآمن والنظيف، والتأكد من خلو سطح المكتب، وكذلك شاشة العرض من المعلومات المصنفة.
٤- تبليغ إدارة الأمن السيبراني عند الاشتباه بأي نشاط قد يتسبب بضرر على أجهزة الحاسب الآلي الخاصة بالأمن العام وأصولها.

الأمن السيبراني المتعلق بالأطراف الخارجية.

لحماية بيانات ومعلومات الأمن العام عند التعامل مع الأطراف الخارجية تم اعتماد سياسة "الامن السيبراني المتعلق بالأطراف الخارجية" والغرض من هذه السياسة هي تحديد الارشادات والمعايير لضمان حماية المعلومات والانظمة عند التعامل مع الاطراف الخارجية وتساعد هذه السياسة في تقليل المخاطر المحتملة وضمان سلامة المعلومات عند التعامل مع الاطراف الخارجية وتنطبق هذه السياسة على جميع الخدمات المقدمة من الأطراف الخارجية وموظفيهم بما في ذلك خدمات الإسناد لتقنية المعلومات والخدمات المدارة للأمن العام، وتنطبق على جميع العاملين (الموظفين والمتعاقدين) في الأمن العام، وتهدف هذه السياسة إلى الآتي:

١- إجراء المسح الأمني (Screening or Vetting) لشركات خدمات الإسناد والخدمات المدارة التي تقدم خدمات لدعم أو تشغيل الأنظمة الحساسة.
٢- التعامل مع أي تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة.
٣- أن تتضمن العقود والاتفاقيات مع الأطراف الخارجية متطلبات الأمن السيبراني للأمن العام وبنود إلزام الأطراف الخارجية بسياسات الأمن السيبراني للأمن العام والمتطلبات التشريعية والتنظيمية ذات العلاقة.
٤- تضمين مسؤوليات الأمن السيبراني وبنود المحافظة على سرية المعلومات (Non-Disclosure Clauses) والحذف الآمن في عقود موظفي الأطراف الخارجية لبيانات الأمن العام (لتشمل خلال وبعد انتهاء/ إنهاء العلاقة الوظيفية مع الأمن العام).
٥- أن تتضمن العقود والاتفاقيات مع الأطراف الخارجية متطلبات خاصة بالأمن السيبراني، بحد أدنى ما يلي:
   i. اتفاقية مستوى الخدمة (SLA).
   ii. إجراءات التعامل في حالة حدوث حادثة أمن سيبراني.
٦- تصنيف بيانات ومعلومات الأمن العام الموجودة في جميع الأنظمة، والتي تُعالجها أو تخزنها الأطراف الخارجية، وفقًا لسياسة تصنيف البيانات والمعلومات المعتمدة في الأمن العام.
٧- عدم نقل بيانات ومعلومات الأمن العام الموجودة في الأنظمة الحسّاسة، والتي تُعالجها أو تخزنها الأطراف الخارجية، خارج بيئة الإنتاج.

الطابعات والماساحات الضوئية وآلات التصوير

لأهمية ضبط التعامل مع الطابعات والماسحات الضوئية وآلات التصوير تم اعتماد سياسة "الأمن السيبراني المتعلق بالطابعات والماساحات الضوئية وآلات التصوير" والغرض من هذه السياسة هو لضمان التعامل الآمن مع البيانات عند استخدام الطابعات والماسحات الضوئية وآلات التصوير وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم 7 - 2 من ضوابط الأمن السيبراني للبيانات، الصادرة من الهيئة الوطنية للأمن السيبراني وتغطي هذه السياسة جميع الأنظمة والأصول المعلوماتية والمعدات والأجهزة الخاصة بوزارة الداخلية وتنطبق على جميع العاملين في الأمن العام ،وتهدف هذه السياسة إلى الآتي:

١- تطبيق متطلبات الأمن السيبراني للطابعات والماسحات الضوئية وآلات التصوير التي تتعامل مع البيانات ذات التصنيف(سري، سري للغاية)بحد أدنى ما يلي:

١,١ تعطيل خاصية التخزين المؤقت.

١,٢ تفعيل خاصية التحقق من الهوية في الطابعات والماسحات الضوئية وآلات التصوير المركزية قبل بدء عمليات الطباعة والتصوير والمسح الضوئي

١,٣ الاحتفاظ بسجل الكتروني للعمليات الخاصة باستخدام الطابعات والماسحات الضوئية وآلات التصوير لفترة لا تقل عن 12 شهر.

١,٤ استخدام أجهزة تمزيق الوثائق الورقية(Cross Shredding) ، لإتلاف الوثائق في حال الانتهاء من استخدامها نهائيا.

تصنيف البيانات

لأهمية حماية البيانات والمعلومات والبيانات التي يتلقاها أو ينتجها أو يتعامل معها الأمن العام مهما كان مصدرها، أو شكلها أو طبيعتها، فقد تم اعتماد "**سياسة تصنيف البيانات**" والتي تهدف إلى تصنيف البيانات وفقاً لحساسيتها وطبيعتها ودرجة أثرها وحسب المبادئ التالية :

المبادئ الرئيسية لتصنيف البيانات:

١. الأصل في البيانات أن تكون متاحة، ما لم تقتض طبيعتها أو حساسيتها مستويات أعلى من التصنيف والحماية.
٢. تصنيف البيانات إلى مستويات وفقا لطبيعتها، ومستوى حساسيتها، ودرجة أثرها مع الأخذ بعين الاعتبار الموازنة بين قيمتها ودرجة سريتها.
٣. تصنيف البيانات عند إنشائها أو حين تلقيها من جهات أخرى ويكون التصنيف خلال فترة زمنية محددة.
٤. اعتماد المستوى الأعلى من التصنيف عندما يتضمن محتوى مجموعة متكاملة من البيانات مستويات تصنيف مختلفة.
٥. الفصل بين مهام ومسؤوليات العاملين - فيما يتعلق بتصنيف البيانات أو الوصول إليها أو الإفصاح عنها أو استخدامها أو التعديل عليها أو إتلافها - بطريقة تحول دون تداخل الاختصاص وتلافي تشتيت المسؤولية.
٦. تقييد الوصول إلى البيانات واستخدامها على أساس الاحتياج الفعلي للمعرفة، ولأقل عدد ممكن من العاملين.
٧. تقييد إدارة صلاحيات العاملين على الحد الأدنى من الامتيازات اللازمة لأداء المهام والمسؤوليات المناطة به.

مستويات تصنيف البيانات

الجدول أدناه يوضح المستويات الرئيسة لتصنيف البيانات بما يتوافق مع مستوى الأثر، كما يوضح بعض الأمثلة الاسترشادية لكل مستوى.

مستوى التصنيف	درجة الأثر	الوصف	أمثلة استرشادية
سري للغاية	**عالي**	تصنف البيانات على أنها «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: ١- سمعة المملكة وبالأمن الوطني، أو سياستها أو مصالحاها أو حقوقها ٢- 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.	• المعلومات العسكرية والأمنية والتحقيقات والعمليات والوقوعات وبيانات الجريمة والحقوقية والمالية. • المعلومات الوثائق التي يتم الحصول عليها بمقتضى اتفاق مع دولة أخرى وتصنف على أنها محمية. • خطط وتفصيلات العمليات العسكرية أو أي معلومات ذات علاقة بها. • المعلومات السياسية الرسمية المتعلقة بالعلاقات الدولية والاتفاقيات. • المعلومات المتعلقة بأعمال وتدابير وتشكيلات الأجهزة الأمنية والاستخباراتية وتجهيزاتها. • معلومات تمس سيادة الدولة.
سري	**متوسط**	تُصنف 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: ١-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. ٢-يحدث خسارة مالية على المستوى التنظيمي تؤدي إلى إفلاس أو عجز الجهات عن أداء مهامها أو خسارة جسيمة للقدرة التنافسية أو كليهما معًا	• معلومات عن مواقع تخزين المواد اللوجستية أو المخازن الاقتصادية. • معلومات متعلقة بالمنشآت الحيوية.هاع • مذكرات التفاهم مع الشركات الدولية لإنشاء مصالح تجارية أو اقتصادية استراتيجية بالمملكة. • معلومات متعلقة بالاتفاقيات الثنائية ومذكرات التفاهم الدبلوماسية بين المملكة والدول الأخرى.
مقيد	**منخفض**	تُصنف البيانات على أنها «مقيّدة»، إذا كان الوصول غير لمصرح به إلى هذه البيانات أو الإفصاح عنها أو عن محتواها يؤدي إلى: ١- تأثير سلبي محدود على عمل الجهات العامة أو الانشطة الاقتصادية في المملكة أو على عمل شخص معين. ٢- ضرر محدود على أصول أي جهة وخسارة محدودة على وضعها المالي والتنافسي.	• معلومات تضر بسمعة أي شخصية عامة. • بيانات مفصلة للمعاملات الفردية. • نتائج الأبحاث والدراسات العلمية قبل نشرها. • المعلومات المتعلقة بالمنتجات تحت التطوير والتي قد تضر بعدالة المنافسة. • معلومات متعلقة بالتعيينات والقرارات الإدارية الحساسة. • تفاصيل تصميم وتطبيق أنظمة أمنية (جدار الحماية، وضوابط الوصول ،ومخططات الشبكة ،وغيرها.) • سياسات وإجراءات الجهات الداخلية رسائل /مذكرات داخلية. • قوائم هواتف داخلية وقوائم البريد الإلكتروني لبعض الجهات.
عام	**لا يوجد**	تُصنف البيانات على أنها «بيانات عامة» عندما لا يترتب على الوصول غير المصرح به إلى هذه البيانات أو الإفصاح عنها أو عن محتواها أي من الآثار المذكورة أعلا ه في حال عدم وجود تأثير على ما يأتي : ١. المصلحة الوطنية ٢. أنشطة الجهات	• توجهات استراتيجية وطنية معلنة. • الإحصاءات الوطنية حول عدد السكان والبيئة والأعمال حسب الصناعة وغيرها. • التنمية العامة والدراسات الاقتصادية. • إجراءات الحكومة وسياستها. • معلومات متعلقة بالخدمات العامة التي تقدمها الحكومة للمواطنين.

حماية البيانات الشخصية

لأهمية حماية البيانات الشخصية وحماية خصوصية الأفراد من خلال تنظيم وجمع ومعالجة وتخزين البيانات الشخصية، فقد تم اعتماد **"سياسة حماية البيانات الشخصية"** والتي تستند إلى ضوابط وسياسات ومعايير تُلزم بحفظ البيانات من أي خرق أو إساءة استخدام، مع ضمان الشفافية والالتزام بالضوابط والسياسات والمعايير.تنطبق أحكام هذه السياسة على جميع جهات الأمن العام، التي تقوم كلياً أو جزئياً بمعالجة البيانات الشخصية، وتهدف السياسة إلى الآتي:

١. حماية حق الأفراد في التعامل الصحيح مع معلوماتهم الشخصية وعدم الكشف عنها.
٢. تجنب إساءة استخدام البيانات الشخصية للأفراد وضمان ثقتهم في الجهة التي تدير بياناتهم.
٣. تمكين الأفراد من الاطلاع والموافقة على من له حق الاطلاع على بياناتهم الشخصية عدا ما نص النظام عليهم.
٤. ضبط آليات الاطلاع على البيانات الشخصية بتوصيف المسوغات النظامية والإجرائية وحدودها.

مشاركة البيانات

لأهمية تنظيم عملية تبادل البيانات والمعلومات بين الأمن العام والجهات المختلفة داخل الإطار القانوني والتشريعي لضمان تحقيق الأهداف المشتركة، عليه فقد تم اعتماد **"سياسة مشاركة البيانات"** وهذه السياسة تركز على ضمان أمان البيانات أثناء المشاركة، مع الالتزام بالشفافية والوضوح في التعامل مع البيانات مع جهات حكومية أخرى أو جهات خاصة أو أفراد - مهما كان مصدر هذه البيانات، أو شكلها أو طبيعتها، وتتضمن هذه السياسة المبادئ الرئيسية لمشاركة البيانات وفق الآتي:

- **المبادئ الرئيسية لمشاركة البيانات :**

١. **مشروعية الغرض:**
مشاركة البيانات تتم فقط لتحقيق أغراض مشروعة ومحددة مسبقًا.
٢. **التوضيح والشفافية:**
ضمان إبلاغ الأطراف المعنية بالغرض من مشاركة البيانات وطريقة استخدامها.
٣. **الوصول المصرح به:**
حصر الوصول إلى البيانات المشتركة على الجهات المصرح لها فقط.
٤. **أمن البيانات:**
اتخاذ تدابير لحماية البيانات المشتركة من أي تهديدات أو اختراقات.
٥. **السرية المُحكمة:**
الحفاظ على سرية البيانات وعدم الإفصاح عنها إلا بما يحقق الغرض من المشاركة.
٦. **أمن البيانات :**
أن تقوم جميع الأطراف المشاركة في مشاركة البيانات بتطبيق الضوابط الأمنية المناسبة لحماية البيانات ومشاركتها في بيئة آمنة وموثوقة وفقاً للأنظمة والتشريعات ذات العلاقة، ووفقاً لما يصدر من الهيئة الوطنية للأمن السيبراني، وإدارة الأمن السيبراني بالأمن العام.