

المملكة الأردنية الهاشمية



المركز الوطني للأمن السيبراني
National Cyber Security Center

**معايير وضوابط الأمن السيبراني للجهات المتعاقدة مع
الوزارات والدوائر الحكومية**
(2023)

الصادرة عن المجلس الوطني للأمن السيبراني بموجب قراره رقم (7) المتخذ في
جلسته المنعقدة بتاريخ 2023/8/9

جدول المحتويات

3	المقدمة.....
3	السند التشريعي وإلزامية التطبيق.....
3	التعاريف.....
4	الغاية والاهداف.....
4	نطاق التطبيق.....
4	الالتزامات لتطبيق الضوابط.....
6	الحوكمة.....

أرقام الصفحات المشمولة بالتعديل	ملخص عن التعديلات	تاريخ الإصدار	رقم الإصدار
-	لا يوجد تعديلات	2023/8/9	1
-			
-			
-			
-			

1. المقدمة

في إطار سعي المركز الوطني للأمن السيبراني إلى بناء منظومة فعالة للأمن السيبراني في المملكة وتطويرها وتنظيمها لحماية المملكة من تهديدات الفضاء السيبراني ومواجهتها بكفاءة وفاعلية بما يضمن استدامة العمل والحفاظ على الأمن الوطني وسلامة الأشخاص والممتلكات والمعلومات، وإيماناً من المركز الوطني للأمن السيبراني بأهمية حماية البيانات الحكومية وتعزيز السيادة على هذه البيانات فقد جاءت هذه الضوابط لحماية البيانات والمعلومات الحكومية بكافة أنواعها وأشكالها ومستوى تصنيفها وفق سياسة تصنيف البيانات الحكومية لعام 2020 الصادرة عن مجلس الوزراء في قراره رقم (8158) تاريخ 2020/1/6 وقانون حماية أسرار ووثائق الدولة رقم 50 لسنة 1971، كما تضمن هذه الضوابط حُسن إدارة أمن المعلومات الحكومية وحمايتها من أي دخول غير مشروع أو غير مصرح به من قبل الجهات المتعاقد معها.

2. السند التشريعي والزامية التطبيق

- استناداً للفقرة (أ) من المادة (4) من قانون الأمن السيبراني التي تنص على (يتولى المجلس المهام والصلاحيات التالية: أ – إقرار الاستراتيجيات والسياسات والمعايير المتعلقة بالأمن السيبراني).
واستناداً لأحكام المادة (8/ب/1) من ذات القانون (تلتزم الوزارات والدوائر الحكومية والمؤسسات الرسمية والعامّة والخاصة والاهلية باتباع السياسات والمعايير والضوابط الصادرة عن المركز لكل قطاع).

3. التعاريف:

أ. يكون للكلمات والعبارات والتالية حيثما وردت في هذه الضوابط المعاني المخصصة لها أدناه ما لم تدل القرينة على غير ذلك:

القانون: قانون الأمن السيبراني رقم 16 لسنة 2019.

المركز: المركز الوطني للأمن السيبراني.

الجهة الحكومية: أي وزارة أو مؤسسة أو دائرة حكومية رسمية أو عامة أو الشركات التي تساهم فيها الحكومة.

الجهة: أي شركة خاصة أو مؤسسة أهلية أو مؤسسة فردية مسجلة في المملكة وفق التشريعات النافذة والتي تقتضي طبيعة تعاملها مع الجهة الحكومية الاطلاع أو الحصول أو إنتاج أو نقل أية معلومات أو بيانات تخص الجهة الحكومية.

البيانات: الأرقام أو الحروف أو الرموز أو الأشكال أو الأصوات أو الصور أو الرسومات التي ليس لها دلالة بذاتها.

المعلومات: البيانات التي تمت معالجتها وأصبح لها دلالة.

المعلومات الحكومية: البيانات والمعلومات العائدة للجهة الحكومية.

4. الغاية والأهداف

تهدف هذه الضوابط إلى:

- أ. حماية المعلومات الحكومية التي قد تطلع عليها أو تنتجها أو تحصل عليها أو تنقلها أي جهة.
- ب. حماية سرية المعلومات الحكومية والحفاظ على سلامتها ومنع تسريبها بأي شكل من الأشكال.
- ج. تعزيز الأمن السيبراني للمعلومات الحكومية وضمان الوصول المنطقي لها ومنع الوصول غير المصرح به.

5. نطاق التطبيق

تطبق هذه الضوابط على كافة الجهات الحكومية والجهات المتعاقد معها.

6. الالتزامات لتطبيق الضوابط

أ. تلتزم الجهة الحكومية عند التعاقد مع أي جهة بما يلي:

1. تطبيق كافة الاحتياطات الأمنية لحماية المعلومات الحكومية الصادرة عن الجهات المعنية بما فيها توقيع اتفاقية عدم الإفصاح مع الجهة المتعاقد معها.
2. الحصول على الموافقات الأمنية اللازمة لموظفي الجهة الذين سيتم اطلاعهم على المعلومات الحكومية ومنحهم صلاحيات الدخول.
3. تدقيق إجراءات الجهة وفحص مدى امتثالها للضوابط والمعايير المطبقة في حال السماح للجهة باستخدام الأجهزة العائدة لها ولموظفيها على شبكة الجهة الحكومية..
4. المراجعة الأمنية وتوثيق أي عملية منح وصول للمعلومات الحكومية تتطابق مع متطلبات العمل وتطبيق مبدأ "صلاحيات الحد الأدنى" وفي حال تطلب الأمر الوصول إلى معلومات أو برمجيات حساسة أو سرية يجب أن يُمنح الوصول لمرة واحدة عند الحاجة وأن يتم إلغاء/تعطيل هذه الصلاحيات بعد الانتهاء من العمل.
5. تحديد المخاطر الأمنية عند شراء المعدات أو الخدمات أو التعاقد مع الجهات لتقديم خدمات أو تزويد معدات أو أنظمة واتخاذ الإجراءات اللازمة لمعالجة هذه المخاطر.
6. إلغاء كافة حسابات المستخدمين المنشأة لغايات استخدام الجهة واسترجاع كافة المعدات والأجهزة المستخدمة في حال تسليمها للجهة.
7. التأكد من أن الجهة قامت بحذف وتدمير كافة المعلومات الحكومية التي تم تزويد الجهة بها حال انتهاء العمل ووفق تعليمات الجهة الحكومية.
8. إضافة نص على العقد المبرم مع الجهة بضرورة التزام الجهة بالضوابط والمعايير الصادرة عن المركز.

ب. تلتزم الجهات المتعاقد معها بما يلي:

1. الامتثال لهذه الضوابط ولقانون الأمن السيبراني وللأنظمة والتعليمات والضوابط والمعايير الصادرة عن المركز.
2. المحافظة على سرية المعلومات الحكومية وتطبيق نظام إدارة أمن المعلومات وأن يتم تبادل البيانات والمعلومات مع الجهة الحكومية وتخزينها بأسلوب التشفير.
3. عدم معالجة أو تخزين أو إرسال أية معلومات حكومية إلى/لدى أي جهة أخرى داخل المملكة إلا بموافقة الجهة الحكومية وإذا كانت الجهة الأخرى خارج المملكة فيجب الحصول على موافقة المركز على ذلك.
4. الالتزام بالصلاحيات الممنوحة من الجهة الحكومية وبالحد الأدنى وعدم تجاوزها.
5. تخزين السجلات الأرشيفية (LOGS) الخاصة بأجهزة الشبكة وأنظمة الحماية على خوادم تابعة للجهة المتعاقد معها أو استضافتها لدى جهة مُرخصة داخل المملكة ولمدة (6 أشهر) على الأقل وبحيث يمكن الوصول إليها عند الحاجة والتأكد من وجود صلاحيات وسيطرة كاملة للجهة عليها.
6. عدم إرسال أي سجلات أرشيفية (LOGS) أو بيانات حكومية حساسة خارج المملكة إلا وفق الإجراءات والشروط الواردة بهذه الضوابط والمعايير.
7. تسليم أية أجهزة محمولة أو أقراص تخزين أو معلومات حكومية عند انتهاء العمل.
8. إتلاف وحذف المعلومات الحكومية وتنفيذ عمليات الإتلاف حسب تعليمات ورقابة الجهة الحكومية والاحتفاظ بسجل لعمليات الإتلاف.
9. إعلام الجهة الحكومية فوراً في حال حدوث حادث أمن سيبراني أو اختراق والتي تقوم بدورها بإبلاغ المركز للتعامل مع الحادث بحسب تصنيفه ومستوى خطورته.

ج. ضوابط التعاقد مع طرف ثالث:

1. عدم التعاقد مع طرف ثالث إلا إذا نص العقد المبرم بين الجهة الحكومية والجهة على ذلك.
2. عدم تبادل المعلومات الحكومية مع الطرف الثالث إلا بما تقتضيه المصلحة وفي حدود العقد المبرم أو بحسب ما تسمح به الجهة الحكومية.
3. يقع على الطرف الثالث ما يقع على الجهة المتعاقد معها من ناحية المسؤوليات والالتزامات الواردة في هذه الوثيقة.
4. لا يُمنح الطرف الثالث إمكانية الوصول إلى المعلومات الحكومية إلا بعد الحصول على الموافقات اللازمة والواردة بهذه الضوابط والمعايير.
5. يلتزم طرفا التعاقد بعمل دراسة تحليل مخاطر والتأكد من المتطلبات الأمنية للموظفين المطلعين على تلك البيانات من الطرف الثالث.

6. توقيع الطرف الثالث على اتفاقية عدم الإفصاح عن المعلومات واتفاقية تحديد مستوى الخدمة (SLA).
7. يجب أن يتضمن العقد مع الطرف الثالث الأدوار والمسؤوليات بما يخص أمن المعلومات وحقوق الملكية الفكرية وغيرها من الحقوق بالإضافة للإجراءات التي سيتم اتخاذها بحق الطرف الثالث في حال عدم الالتزام بنود العقد.
8. تلتزم الجهة الحكومية مراجعة العقود المبرمة مع الطرف الثالث وعرضها على مديرية/ وحدة الشؤون القانونية لديها وفي حال كان الطرف الثالث أجنبياً التأكد من انسجام العقد مع القوانين والتشريعات الأردنية.
9. ضرورة إعلام الطرف الثالث بالإبلاغ عن أي خرق أو حادث أمن سيبراني للبيانات الحكومية تحت طائلة المساءلة القانونية.

7. الحوكمة

يتولى المركز مراقبة مدى التزام الجهات والجهات الحكومية بهذه الضوابط والمعايير واتخاذ الإجراء المناسب في حال عدم الالتزام.