شركة الكهرباء الوطنية

السياسة العامة للأمن السيبراني

قائمة تعديلات الوثيقة

معلومات النسخة						اعتماد النسخة		
#	رقم النسخة	التعديل	الإعداد	التاريخ	رئيس قسم الأمن السيبراني	مدير الدائرة المعنية	المدير العام
1	Rev 1.0		أحمد بطاينه	2024/5/26			

قائمة المحتويات

الغاية 3
نطاق التطبيق 3
الأدوار والمسؤوليات 3
بنود السياسة. 4

الغاية

تهدف السياسة العامة إلى تأطير أعمال الأمن السيبراني في شركة الكهرباء الوطنية من أجل حماية المعلومات وأنظمتها الرقمية الخاصة بالشركة من التهديدات السيبرانية الداخية والخارجية المحتملة، وذلك عن طريق بناء منظومة فعالة للأمن السيبراني وتطويرها وتنظيمها لحماية الشركة من تهديدات الفضاء السيبراني, والتأكد من الإمتثال للقوانين والأنظمة والتشريعات المحلية ذات الصلة واتباع أفضل الممارسات العالمية في مجال حماية المعلومات.

وتعتبر السياسة العامة المرجع الرئيسي لسياسات الأمن السيبراني التنظيمية واجراءاته.

نطاق التطبيق

يتم تطبيق السياسة العامة للأمن السيبراني على جميع الأصول الرقمية في شركة الكهرباء الوطنية بكل ما يتعلق بأنظمة وتقنيات المعلومات الرقمية والمتصلة بشبكة نقل معلومات، من ناحية ادارة أو نقل أو تخزين أو معالجة أو جلب أو مشاركة المعلومات داخل الشركة أو خارجها.

بحيث تشمل الأصول الرقمية، الأجهزة والمعدات والأنظمة والخدمات والبيانات بشتى أشكالها الرقمية، وتشمل شبكات المعلومات الشبكات التي تخدم أنظمة تقنيات المعلومات (IT) أو أنظمة التقنيات التشغيلية (OT).

كما تنطبق السياسة على جميع العاملين (موظفين ومتعاقدين) والجهات والأطراف الخارجية التي تتعامل مع الشركة.

الأدوار والمسؤوليات

1. يتم اعتماد السياسة العامة والسياسات التنظيمية الأخرى للأمن السيبراني من قبل عطوفة المدير العام ليتم بعد ذلك مشاركتها عبر الوسائل المناسبة للأطراف الداخلية والخارجية ذات العلاقة.
2. يقوم قسم الأمن السيبراني بإعداد ونشر سياسات الأمن السيبراني العامة والتنظيمية و مراجعتها مع المعنيين وتحديثها باستمرار.
3. يقوم قسم الأمن السيبراني بتنفيذ النشاطات والعمليات التشغيلية للأمن السيبراني المحددة ضمن محاور برنامج الأمن السيبراني.
4. تقوم الوحدات الإدارية بالتأكد من أن إجراءات العمل لديها تتوافق مع سياسات الأمن السيبراني عند القيام بأي تغيير على وضع قائم للأصول الرقمية التي تديرها او تتعامل معها.

5. تقوم الوحدات الإدارية المعنية بإعداد قائمة أصول الأنظمة الرقمية التي تقع تحت مسؤوليتها وتحديثها كلما لزم الأمر وإرسالها إلى قسم الأمن السيبراني.
6. يقوم قسم الأمن السيبراني بتقييم المخاطر ومراجعتها بشكل دوري استنادا إلى قائمة أصول الأنظمة الرقمية وما يجري عليها من تغيير لوضع قائم.
7. يقوم قسم الأمن السيبراني بدراسة وإعداد الضوابط الفنية والتنظيمية التي تهدف إلى حماية الأنظمة الرقمية وذلك اعتمادا على إدارة المخاطر والتأكد من الامتثال للقوانين والتشريعات ومقاييس الأمن السيبراني ذات الصلة. وتدقيق تطبيق ضوابط الأمن السيبراني وتوثيقها.
8. تقوم الوحدات الإدارية المعنية بتطبيق الضوابط الفنية والتنظيمية والالتزام بأدوارها ومسؤولياتها حسب سياسات الأمن السيبراني العامة والتنظيمية.
9. يقوم قسم الأمن السيبراني بنشر الوعي بالتهديدات السيبرانية وطرق التعامل معها، ومشاركة الحوادث السيبرانية التي حدثت أو كان من المتوقع حدوثها مع المعنيين للاستفادة منها ولضمان التحسين المستمر.
10. من مسؤولية العاملين في الشركة والوحدات الإدارية الابلاغ عن الحوادث السيبرانية عند حصول (أو الشك بحصول) أي تهديد أو حادث سيبراني يتعلق بالشركة.
11. يحق لقسم الأمن السيبراني الاطلاع على المعلومات وجمع الأدلة اللازمة؛ للتأكد من الالتزام بالمتطلبات التشريعية والتنظيمية ذات العلاقة.

بنود السياسة:

ينبثق من السياسة العامة للأمن السيبراني سياسات أمنية تنظيمية وتشغيلية مفصلة تعمل على تأطير الضوابط والتدابير الفنية والتنظيمية لأعمال الأمن السيبراني ضمن سياسات مرجعية تلتزم بها الوحدات الإدارية المعنية بما يتلائم مع هدف ومضمون كل سياسة. وتشمل السياسات الأمنية التالية:

1. **سياسة الأمن السيبراني للمشاريع الرقمية والتقنية**

   تهدف إلى ادماج متطلبات الأمن السيبراني في مشاريع غايتها تقنية المعلومات (IT) أو مشاريع غايتها التقنيات التشغيلية (OT) أو مشاريع لها غايات أخرى لكنها تتضمن تقنيات رقمية وتقنية. وتسعى هذه السياسة إلى تحديد المتطلبات السيبرانية لتغطي مراحل المشروع بهدف حماية سرية المعلومات، وسلامة الأصول الرقمية وضمان دقتها وتوافرها.

2. **سياسة حماية البريد الإلكتروني**

   تهدف السياسة لضمان حماية خدمة البريد الإلكتروني لشركة الكهرباء الوطنية من المخاطر السيبرانية.

3. **سياسة إدارة أمن شبكات تقنية المعلومات**

تهدف السياسة لضمان حماية شبكة تقنية المعلومات (IT) لشركة الكهرباء الوطنية وحماية طرق الاتصال بها من المخاطر السيبرانية.

4. **سياسة أمن الخوادم**

تهدف السياسة لضمان حماية الخوادم العاملة في شبكة تقنية المعلومات (IT) لشركة الكهرباء الوطنية من المخاطر السيبرانية.

5. **سياسة إدارة حزم التحديثات والإصلاحات**

تهدف السياسة إلى ضبط وإدارة حزم التحديثات الممكنة لأنظمة التشغيل والأجهزة والبرمجيات في شركة الكهرباء الوطنية لحمايتها من المخاطر السيبرانية.

6. **سياسة أمن قواعد البيانات**

تهدف السياسة لضمان حماية أنظمة قواعد البيانات لشركة الكهرباء الوطنية من المخاطر السيبرانية.

7. **سياسة النسخ الاحتياطي**

تهدف السياسة لتحديد متطلبات الأمن السيبراني المتعلقة بالنسخ الاحتياطي للأصول الرقمية والبيانات لتقليل المخاطر السيبرانية.

8. **سياسة الأمن السيبراني للأطراف الخارجيين (Third-Party Cybersecurity)**

تهدف السياسة إلى تحديد متطلبات الأمن السيبراني المتعلقة بالأطراف الخارجيين سواء أكانوا شركات أم أفراد لمن لهم علاقة عمل بشركة الكهرباء الوطنية من أجل تقليل المخاطر السيبرانية.

9. **سياسة الأمن السيبراني للأنظمة التشغيلية**

تهدف السياسة إلى ضمان توفير الحماية الفعالة من المخاطر السيبرانية لأنظمة التقنيات التشغيلية العاملة في شركة الكهرباء الوطنية بمختلف أشكالها والتي يمكن من خلالها الاتصال بمكونات النظام الكهربائي وتنفيذ أوامر تشغيلية على النظام (Control) أو مراقبة (Monitor) مكونات النظام الكهربائي.

10. **سياسة التوعية والتدريب بالأمن السيبراني**

تهدف السياسة إلى تحديد متطلبات وآليات رفع مستوى الوعي والمهارات بالأمن السيبراني للعاملين في شركة الكهرباء الوطنية وضمان معرفة الموظفين بمسؤولياتهم وأدوارهم في برنامج الأمن السيبراني.

11. **سياسة الاستخدام الآمن والمقبول للأصول الرقمية**

تهدف السياسة إلى تحديد متطلبات الأمن السيبراني المتعلقة بآليات الاستخدام الآمن من قبل العاملين في شركة الكهرباء الوطنية للأجهزة الحاسوب وملحقاتها والأنظمة والخدمات الرقمية الداخلية والخارجية المتاحة عبر شبكات نقل المعلومات في شركة الكهرباء الوطنية.