دورة تدريبية: حوكمة الأمن السيبراني

تطبيق ضوابط ومعايير الهيئة الوطنية للأمن السيبراني

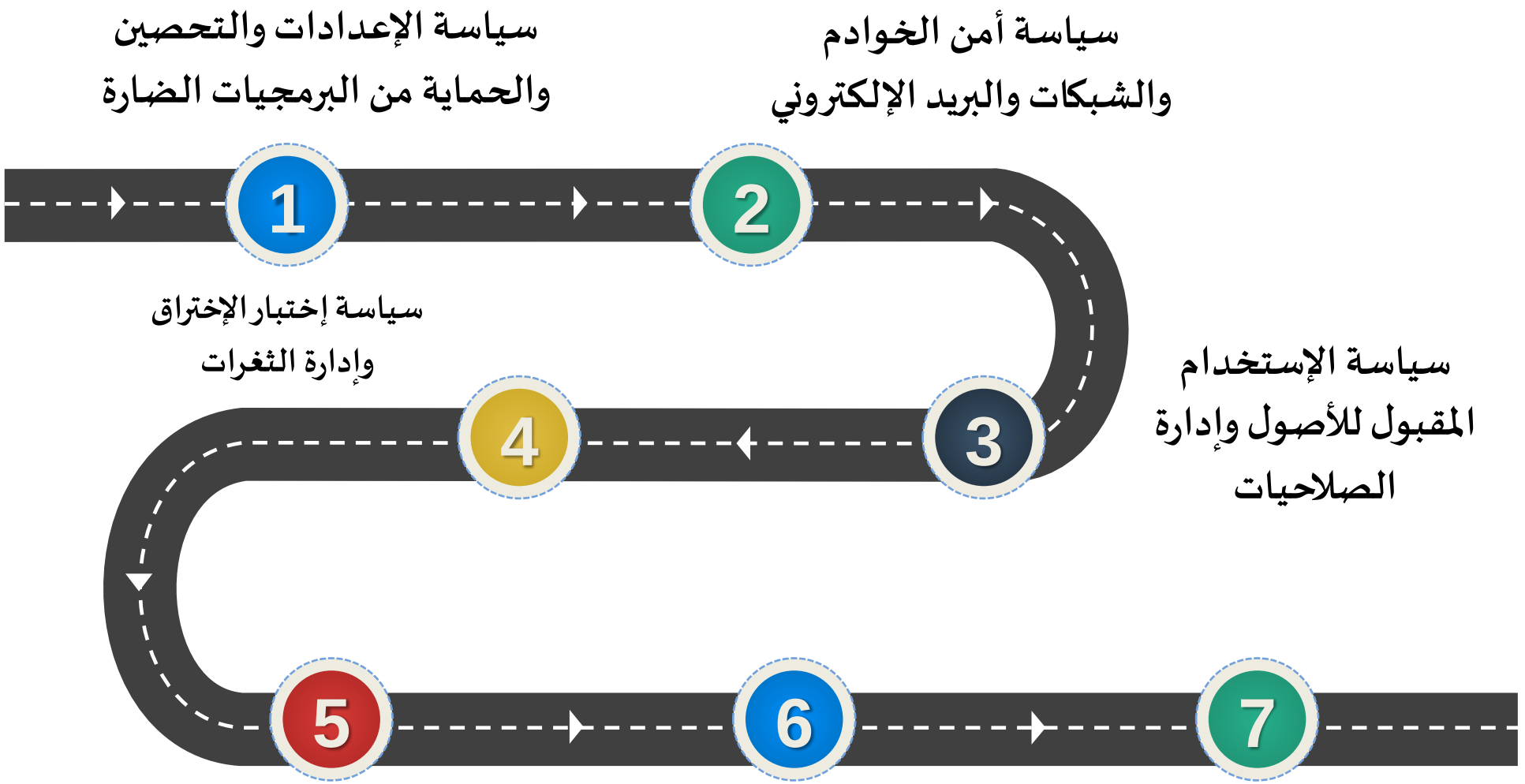
المحاضرة السابعة (الجزء الثاني)

د. غالب الشمري

أستاذ الذكاء الإصطناعي وعلم البيانات المساعد

جامعة الملك سعود

خارطة الطريق



عصف ذهني

من وجهة نظرك
ما هي ضوابط الأمن السيبراني
لإعدادات التحصين والحماية من
البرمجيات الضارة؟

سياسة الإعدادات والتحصين

تهدف هذه السياسة إلى توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية وتحصين وضبط إعدادات الأصول المعلوماتية والتقنية والتطبيقات الخاصة بالجهة لمقاومة الهجمات السيبرانية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها. كما تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-٦-٢-٢ والضابط رقم ١-٦-٣-٥ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة عن الهيئة الوطنية للأمن السيبراني.

بنود السياسة:

- يجب تحديد جميع الأصول المعلوماتية والتقنية المستخدمة داخل الجهة، وكذلك التطبيقات والبرمجيات المعتمدو والتأكيد من توفير معايير تقنية أمنية لها.
- يجب تطوير وتوثيق واعتماد المعايير التقنية الأمنية الخاصة بجميع الأصول المعلوماتية والتقنية والتطبيقات والبرمجيات المصرح بها داخل الجهة.

سياسة الإعدادات والتحصين

بنود السياسة:

- يجب تحصين وضبط إعدادات أجهزة الحاسب الآلي، والأنظمة، والتطبيقات، وأجهزة الشبكات، والأجهزة الأمنية الخاصة بالجهة بما يتوافق مع المعايير التقنية الأمنية المعتمدة لمقاومة الهجمات السيبرانية.
- يجب إستخدام إحدى طرق التالية لتطوير المعايير الأمنية التقنية:
  - دليل الإعدادات والتحصين الخاصة بالموارد وذلك وفقاً للسياسات والإجراءات التنظيمية الخاصة بالجهة والمتطلبات التشريعية والتنظيمية وأفضل الممارسات العالمية.
  - دليل الإعدادات والتحصين من مصادر موثوقة ومتوافقة مع المعايير المصنعية، مثل: مركز أمن الأنترنت CIS، ومعهد الأمن والشبكات وإدارة النظم SANS، والمعهد الوطني للمعايير والتقنية NIST، ووكالة أنظمة معلومات الدفاع DISA وغيرها.
  - تطوير معايير أمنية تقنية خاصة بالجهة بما يتناسب مع طبيعة الأعمال وبما يتوافق مع دليل الإعدادات والتحصين الخاص بالموارد والمعايير المصنعية.

سياسة الإعدادات والتحصين

بنود السياسة:

- يجب أن تغطي الضوابط الخاصة بالمعايير التقنية الأمنية بحد أدنى ما يلي:
  - إيقاف أو تغيير الحسابات المصنعية والإفتراضية
  - منع تثبيت البرمجيات الغير مرغوب بها
  - تعطيل منافذ الشبكة الغير مستخدمة
  - تقييد إستخدام وسائط الحفظ والتخزين الخارجي
  - تغيير الإعدادات الإفتراضية التي قد تُستغل في الهجمات السيبرانية
- يجب مراجعة الإعدادات والتحصين والتأكد من تطبيقها في الحالات التالية:
  - مراجعة إعدادات الأصول المعلوماتية والتقنية دورياً
  - مراجعة الإعدادات والتحصين قبل إطلاق وتدشين المشاريع والتغييرات المتعلقة بالأصول والتطبيقات
  - مراجعة الإعدادات والتحصين لأنظمة التحكم الصناعي بشكل دوري والتأكد من تطبيقها كافة المعايير الأمنية

سياسة الإعدادات والتحصين

بنود السياسة:

- يجب إعتماد صورة لإعدادات وتحصين الأصول المعلوماتية والتقنية الخاصة بالجهة وفقاً لكافة المعايير الأمنية.
- يجب إستخدام صورة معتمدة في تثبيت أو تحديث الأصول المعلوماتية والتقنية
- يجب توفير التقنيات اللازمة لإدارة الإعدادات والتحصين مركزياً، والتأكد من إمكانية تطبيق أو تحديث الإعدادات والتحصين تلقائياً لكافة الأصول المعلوماتية والتقنية في مواعيد زمنية محددة ومخطط لها.
- يجب توفير نظام مراقبة الإعدادات المتوافقة مع «بروتوكول أتمتة المحتوى الأمني» للتأكد من أن الإعدادات متوافقة مع المعايير التقنية الأمنية المعتمدة ومطبقة بشكل كامل، كما يجب الإبلاغ عن أي تغييرات غير مصرّح بها.
- يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لإدارة الإعدادات والتحصين.
- يجب مراجعة متطلبات الأمن السيبراني المتعلقة بالإعدادات والتحصين للأصول المعلوماتية والتقنية والتطبيقات الخاصة بالجهة سنوياً، أو في حالة حدوث تغييرات في المتطلبات التشريعية أو التنظيمية أو المعايير ذات العلاقة.

سياسة الحماية من البرمجيات الضارة

تهدف هذه السياسة إلى توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية أجهزة المستخدمين والأجهزة المحمولة والخوادم الخاصة بالجهة من تهديدات البرمجيات الضارة وتقليل المخاطر السيبرانية الناتجة عن التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها. كما تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

بنود السياسة:

- يجب على الجهة تحديد تقنيات وآليات الحماية الحديثة والمتقدمة وتوفيرها والتأكد من موثوقيتها.
- يجب تطبيق تقنيات وآليات الحماية لحماية أجهزة المستخدمين والأجهزة المحمولة والخوادم من البرمجيات الضارة وإدراتها بشكل آمن.

سياسة الحماية من البرمجيات الضارة

بنود السياسة:

- يجب التأكد من أن تقنيات وآليات الحماية قادرة على اكتشاف جميع أنواع البرمجيات الضارة المعروفة وإزالتها، مثل الفيروسات (Virus)، وأحصنة طروادة (Trojan Horse)، والديدان (Worms)، وبرمجيات التجسس (Spyware)، وبرمجيات الإعلانات المتسللة (Adware)، ومجموعة الجذر (Root Kits).
- قبل اختيار تقنيات وآليات الحماية، يجب التأكد من ملاءمتها لأنظمة التشغيل الخاصة بالجهة مثل أنظمة ويندوز (Windows)، وأنظمة يونكس (UNIX)، وأنظمة لينكس (Linux)، ونظام ماك (Mac)، وغيرها.
- في حال تسبب تحديث تقنيات الحماية بضرر للأنظمة أو متطلبات الأعمال، يجب التأكد من أن تقنيات الحماية قابلة للاسترجاع إلى النسخة السابقة.
- يجب تقييد صلاحيات تعطيل التثبيت أو إلغائه أو تغيير إعدادات تقنيات الحماية من البرمجيات الضارة ومنحها لمشرفي نظام الحماية فقط.

عصف ذهني

من وجهة نظرك
ما هي ضوابط الأمن السيبراني
لسياسة أمن الخوادم والشبكات
والبريد الإلكتروني؟

سياسة أمن الخوادم

تهدف هذه السياسة إلى توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بالخوادم (Servers) الخاصة بالجهة لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها. كما تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

بنود السياسة:

- يجب تحديد جميع الخوادم الخاصة بالجهة وتوثيقها والتأكد من أن برمجيات الخوادم محدثة ومعتمدة.
- يجب تطوير وتطبيق معايير تقنية أمنية Technical Security Standards للخوادم المستخدمة داخل الجهة بإستخدام أفضل المعايير العالمية.

سياسة أمن الخوادم

بنود السياسة:

- يجب ضبط إعدادات الخوادم وفقاً للمعايير التقنية الأمنية المعتمدة قبل تشغيل الخوادم في بيئة الإنتاج.
- يجب توفير الحماية اللازمة لجميع الخوادم للسيطرة على مخاطر الأمن السيبراني ذات العلاقة.
- يجب عمل نسخ احتياطية منتظمة للخوادم وفقاً لسياسة إدارة النسخ الاحتياطية المعتمدة في الجهة لضمان إمكانية استعادتها في حال تعرّضها لتلف أو حادث غير مقصود. (توصي الهيئة بعمل نسخ احتياطية يومياً للأنظمة الحساسة).
- يجب تحديث برمجيات الخوادم بما في ذلك أنظمة التشغيل وبرامج التطبيقات وتزويدها بأحدث حزم التحديثات والإصلاحات الأمنية وفقاً لسياسة إدارة التحديثات والإصلاحات المعتمدة في الجهة.

سياسة أمن الشبكات

تهدف هذه السياسة إلى توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بأمن الشبكات الخاصة بالجهة لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها. كما تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-٥-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

بنود السياسة:

- تحديد وتوثيق جميع أجهزة الشبكة داخل الجهة والتأكد من أن جميع الأجهزة محدثة ومعتمدة.
- توثيق واعتماد معايير تقنية أمنية (Technical Security Standards) لجميع أجهزة الشبكة المستخدمة داخل الجهة.
- إدارة صلاحيات الدخول إلى الشبكات الخاصة بالجهة وفقاً لسياسة إدارة هويات الدخول والصلاحيات، بحيث يكون الاتصال بالشبكة متوفراً عند الحاجة ومتاحاً للمستخدمين المصرح لهم فقط.

عصف ذهني

من وجهة نظرك

- ما هي متطلبات الوصول للشبكة؟
- ما هي متطلبات وصول الأطراف الخارجية؟
- ما هي متطلبات حماية الشبكات؟
- ما هي متطلبات الأمن المادي والبيئي؟

سياسة أمن البريد الإلكتروني

تهدف هذه السياسة إلى توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لتقليل المخاطر السيبرانية الناتجة عن إستخدام الجهة للبريد الإلكتروني وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية، سلامة، وتوافر خدمة البريد الإلكتروني. كما تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة وأفضل الممارسات العالمية، وهي مطلب تشريعي في الضابط رقم ٢-٤-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

بنود السياسة:

- يجب توفير تقنيات حديثة لحماية البريد الإلكتروني وتحليل وتصفية (Filtering) رسائل البريد الإلكتروني وحظر الرسائل المشبوهة، مثل الرسائل الاقتحامية (Spam Emails) ورسائل التصيّد الإلكتروني (Phishing Emails).
- يجب أن تستخدم أنظمة البريد الإلكتروني أرقام تعريف المستخدم وكلمات المرور مرتبطة، لضمان عزل اتصالات المستخدمين المختلفين.

سياسة أمن البريد الإلكتروني

بنود السياسة:

- يجب توفير التقنيات اللازمة لتشفير البريد الإلكتروني الذي يحتوي على معلومات مصنفة.
- يجب تطبيق خاصية التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) للدخول عن بعد والدخول عن طريق صفحة موقع البريد الإلكتروني (Webmail).
- يجب أرشفة رسائل البريد الإلكتروني والقيام بالنسخ الاحتياطي دورياً.
- يجب تحديد مسؤولية البريد الإلكتروني للحسابات العامة والمشتركة (Generic Account)
- يجب توفير تقنيات الحماية اللازمة من الفيروسات، والبرمجيات الضارة غير المعروفة مسبقا (Zero-Day Protection) على خوادم البريد الإلكتروني؛ والتأكد من فحص الرسائل قبل وصولها لصندوق بريد المستخدم.
- يجب توثيق مجال البريد الإلكتروني للجهة عن طريق استخدام الوسائل اللازمة، مثل طريقة إطار سياسة مرسل البريد الإلكتروني (Sender Policy Framework) لمنع تزوير البريد الإلكتروني (Email Spoofing). كما يجب التأكد من موثوقية مجالات رسائل البريد الواردة (Incoming message DMARC verification).

سياسة أمن البريد الإلكتروني

بنود السياسة:

- يجب أن يقتصر الوصول إلى رسائل البريد الإلكتروني على العاملين لدى الجهة.
- يجب اتخاذ الإجراءات اللازمة؛ لمنع استخدام البريد الإلكتروني للجهة في غير أغراض العمل.
- يمنع وصول مسؤول النظام (System Administrator) إلى معلومات البريد الإلكتروني الخاصة بأي موظف دون الحصول على تصريح مسبق.
- يجب تحديد حجم مرفقات البريد الإلكتروني الصادر والوارد، وسعة صندوق البريد لكل مستخدم. وكذلك العمل على الحد من إتاحة إرسال الرسائل الجماعية لعدد كبير من المستخدمين.
- يجب تذييل رسائل البريد الإلكتروني المرسلة إلى خارج الجهة بإشعار إخلاء المسؤولية.
- يجب تطبيق التقنيات اللازمة؛ لحماية سرية رسائل البريد الإلكتروني وسلامتها، وتوافرها أثناء نقلها وحفظها؛ وتشمل هذه الإجراءات استخدام تقنيات التشفير وتقنيات منع تسريب البيانات.
- يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لنظام البريد الإلكتروني.

يجب تعطيل خدمة تحويل البريد الإلكتروني من الخادم (Open Mail Relay).

عصف ذهني

من وجهة نظرك
ما هي ضوابط الأمن السيبراني
لسياسة الإستخدام المقبول للأصول
وإدارة الصلاحيات؟

سياسة الإستخدام المقبول للأصول

تهدف هذه السياسة إلى توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لتقليل المخاطر السيبرانية المتعلقة بإستخدام أنظمة الجهة وأصولها، وحمايتها من التهديدات الداخلية والخارجية، والعناية بالأهداف الأساسية للحماية وهي: سرية، سلامة، وتوافر المعلومات. كما تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة وأفضل الممارسات العالمية، وهي مطلب تشريعي في الضابط رقم ٢-١-٣ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

بنود السياسة:

- يجب التعامل مع المعلومات حسب التصنيف المحدد، وبما يتوافق مع سياسة تصنيف البيانات وسياسة حماية البيانات والمعلومات الخاصة بالجهة بشكل يضمن حماية سرية المعلومات وسلامتها وتوافرها.
- يحظر انتهاك حقوق أي شخص، أو شركة محمية بحقوق النشر، أو براءة الاختراع، أو أي ملكية فكرية أخرى، أو قوانين أو لوائح مماثلة؛ بما في ذلك، على سبيل المثال لا الحصر، تثبيت برامج غير مصرح بها أو غير قانونية.

سياسة الإستخدام المقبول للأصول

بنود السياسة:

- يجب عدم ترك المطبوعات على الطابعة المشتركة دون رقابة.
- يجب حفظ وسائط التخزين الخارجية بشكل آمن وملائم، مثل التأكد من ضبط درجة الحرارة بدرجة معينة، وحفظها في مكان معزول وآمن.
- يمنع استخدام كلمة المرور الخاصة بمستخدمين آخرين، بما في ذلك كلمة المرور الخاصة بمدير المستخدم أو مرؤوسيه.
- يجب الالتزام بسياسة المكتب الآمن والنظيف، والتأكد من خلو سطح المكتب، وكذلك شاشة العرض من المعلومات المصنفة.
- يمنع الإفصاح عن أي معلومات تخص الجهة، بما في ذلك المعلومات المتعلقة بالأنظمة والشبكات لأي جهة أو طرف غير مصرح له سواءً كان ذلك داخلياً أو خارجياً.
- يُمنع نشر معلومات تخص الجهة عبر وسائل الإعلام، وشبكات التواصل الاجتماعي دون تصريح مسبق.

يُمنع استخدام أنظمة الجهة وأصولها بغرض تحقيق منفعة وأعمال شخصية، أو تحقيق أي غرض لا يتعلق بنشاط وأعمال الجهة.

سياسة الإستخدام المقبول للأصول

بنود السياسة:

- يُمنع ربط الأجهزة الشخصية بالشبكات، والأنظمة الخاصة بالجهة دون الحصول على تصريح مسبق، وبما يتوافق مع سياسة أمن الأجهزة المحمولة (BYOD).
- يُمنع القيام بأي أنشطة تهدف إلى تجاوز أنظمة الحماية الخاصة بالجهة، بما في ذلك برامج مكافحة الفيروسات، وجدار الحماية، والبرمجيات الضارة دون الحصول على تصريح مسبق، وبما يتوافق مع الإجراءات المعتمدة لدى الجهة.
- تحتفظ إدارة الأمن السيبراني بحقها في مراقبة الأنظمة والشبكات والحسابات الشخصية المتعلقة بالعمل، ومراجعتها دورياً لمراقبة الالتزام بسياسات الأمن السيبراني ومعاييره.
- يُمنع استضافة أشخاص غير مصرح لهم بالدخول للأماكن الحساسة دون الحصول على تصريح مسبق.
- يجب ارتداء البطاقة التعريفية في جميع مرافق <الجهة.
- يجب تبليغ إدارة الأمن السيبراني في حال فقدان المعلومات أو سرقتها أو تسريبها.

سياسة إدارة هويات الدخول والصلاحيات

تهدف هذه السياسة إلى توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بإدارة هويات الدخول والصلاحيات على الأصول المعلوماتية والتقنية الخاصة بالجهة لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية، والعناية بالأهداف الأساسية للحماية وهي: سرية، سلامة، وتوافر المعلومات. كما تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة وأفضل الممارسات العالمية، وهي مطلب تشريعي في الضابط رقم ٢-٢-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

بنود السياسة:

- إدارة هويات الدخول والصلاحيات
- مراجعة هويات الدخول والصلاحيات
- إدارة كلمات المرور
- متطلبات أخرى

نموذج-سياسة-إدارة-هويات-الدخول-والصلاحيات

عصف ذهني

من وجهة نظرك
ما هي ضوابط الأمن السيبراني لسياسة إختبار الإختراق وإدارة الثغرات؟

سياسة إختبار الإختراق

تهدف هذه السياسة إلى توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بتقييم وأختبار مدى فعالية قدرات تعزيز الأمن السيبراني في الجهة وذلك من خلال محاكاة تقنيات وأساليب الهجوم السيبراني الفعلية، لإكتشاف نقاط الضعف الأمنية الغير معروفة والتي تؤدي إلى الإختراق السيبراني للجهة ولتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية، والعناية بالأهداف الأساسية للحماية وهي: سرية، سلامة، وتوافر المعلومات. كما تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة وأفضل الممارسات العالمية، وهي مطلب تشريعي في الضابط رقم ٢-١١-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

بنود السياسة:

- يجب على الجهة إجراء إختبار الإختراق دورياً، لتقييم وإختبار مدى فعالية قدرات تعزيز الأمن السيبراني.
- تحدد إدارة الأمن السيبراني الأنظمة والخدمات والمكونات التقنية التي يجب إجراء إختبار الإختراق عليها وفقاً للمتطلبات التشريعية والتنظيمية.
- يجب على الجهة إجراء إختبار الإختراق على جميع الخدمات المقدمة خارجياً ومكوناتها التقنية دورياً.

سياسة إختبار الإختراق

بنود السياسة:

- يجب التأكد من أن اختبار الاختراق لا يؤثر على الأنظمة والخدمات المقدمة في الجهة.
- يجب على الجهة إجراء اختبار الاختراق على الأنظمة الحساسة ومكوناتها التقنية كل ستة أشهر؛ على الأقل. (CSCC-2-10-2)
- يجب إجراء اختبار الاختراق لاكتشاف نقاط الضعف الأمنية بكافة صورها والتي تشمل نقاط الضعف التي تنتج عادةً عن أخطاء في تطوير التطبيقات (Application Development Error) وضبط إعدادات النظام بشكل غير آمن (Configurations Faults) وإمكانية استغلال ثغرة محددة (Exploitability of Identified Vulnerability).
- يجب تطوير إجراءات خاصة باختبار الاختراق واعتمادها ونشرها، مع الأخذ بالاعتبار عدم تأثيرها على سير الأعمال الخاصة بالجهة.
- يجب على إدارة الأمن اليبراني تحديد أو الموافقة على أساليب اختبار الاختراق والأدوات والتقنيات التي يستخدمها فريق اختبار الاختراق الداخلي أو الخارجي قبل بدء عملية اختبار الاختراق.
- في حال تفويض طرف خارجي للقيام باختبار الاختراق نيابة عن الجهة، يجب التحقق من تطبيق جميع متطلبات الأمن السيبراني المتعلقة بالأطراف الخارجية ووفقاً لسياسة الأمن السيبراني المتعلّق بالأطراف الخارجية المعتمدة في الجهة.
- يجب تصنيف نتائج اختبار الاختراق بناءً على خطورتها، ومعالجتها حسب المخاطر السيبرانية المترتبة عليها ووفقاً لمنهجية إدارة المخاطر المعتمدة لدى الجهة.
- يجب وضع خطة عمل لمعالجة نتائج اختبار الاختراق يوضح فيها تأثير المخاطر وآلية معالجتها والمسؤول عن تطبيقها والفترة الزمنية اللازمة لتنفيذها.

سياسة إدارة الثغرات

تهدف هذه السياسة إلى توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لضمان إكتشاف الثغرات التقنية في الوقت المناسب ومعالجتها بشكل فعال، وذلك لمنع إحتمالية إستغلال هذه الثغرات من قبل الهجمات السيبرانية أو تقليلها، وكذلك التقليل من الآثار المترتبة على أعمال الجهة وحمايتها من التهديدات الداخلية والخارجية، والعناية بالأهداف الأساسية للحماية وهي: سرية، سلامة، وتوافر المعلومات. كما تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة وأفضل الممارسات العالمية، وهي مطلب تشريعي في الضابط رقم ٢-١٠-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

بنود السياسة:

- المتطلبات العامة
- متطلبات تقييم الثغرات
- متطلبات معالجة الثغرات
- متطلبات أخرى

عصف ذهني

من وجهة نظرك
ما هي ضوابط الأمن السيبراني
لسياسة أمن قواعد البيانات
وتطبيقات الويب؟

سياسة أمن قواعد البيانات

تهدف هذه السياسة إلى توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية قواعد البيانات Database الخاصة بالجهة وذلك من خلال محاكاة تقنيات وأساليب الهجوم السيبراني الفعلية، لإكتشاف نقاط الضعف الأمنية الغير معروفة والتي تؤدي إلى الإختراق السيبراني للجهة ولتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية، والعناية بالأهداف الأساسية للحماية وهي: سرية، سلامة، وتوافر المعلومات. كما تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة وأفضل الممارسات العالمية، وهي مطلب تشريعي في الضابط رقم ١-٣-٢ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

بنود السياسة:

- البنود العامة
- الإجراءات الأمنية المطلوبة لإستضافة قواعد البيانات
- المتطلبات المتعلقة بإدارة التغييرات على أنظمة قواعد البيانات
- مراقبة سجلات الأحداث المتعلقة بنظام قواعد البيانات
- المتطلبات التشغيلية
- متطلبات أخرى

سياسة أمن تطبيقات الويب

تهدف هذه السياسة إلى توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية تطبيقات الويب الخارجية الخاصة بالجهة وذلك من خلال محاكاة تقنيات وأساليب الهجوم السيبراني الفعلية، لإكتشاف نقاط الضعف الأمنية الغير معروفة والتي تؤدي إلى الإختراق السيبراني للجهة ولتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية، والعناية بالأهداف الأساسية للحماية وهي: سرية، سلامة، وتوافر المعلومات. كما تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة وأفضل الممارسات العالمية، وهي مطلب تشريعي في الضابط رقم ٢-١٥-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

بنود السياسة:

- المتطلبات العامة
- متطلبات حق الوصول
- متطلبات تطوير أو شراء تطبيقات الويب
- متطلبات أخرى

عصف ذهني

من وجهة نظرك
ما هي ضوابط الأمن السيبراني
لسياسة مراجعة وتدقيق الأمن
السيبراني وسياسة الموارد البشرية؟

سياسة مراجعة وتدقيق الأمن السيبراني

تهدف هذه السياسة إلى توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة لمراجعة وتدقيق ضوابط الأمن السيبراني لدى الجهة والتأكد من تطبيقها وأنها تعمل وفقاً للسياسات والإجراءات التنظيمية للجهة والمتطلبات التشريعية والتنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المُقرة تنظيمياً على الجهة. كما تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة وأفضل الممارسات العالمية، وهي مطلب تشريعي في الضابط رقم ١-٨-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

بنود السياسة:

- يجب على إدارة الأمن السيبراني مراجعة تطبيق ضوابط الأمن السيبراني دورياً، ومراجعة مدى الإلتزام بالضوابط الأساسية للأمن السيبراني ECC:1-2018 وضوابط الأمن السيبراني للأنظمة الحساسة CSCC-1:2019
- يجب مراجعة وتدقيق تطبيق ضوابط الأمن السيبراني درورياً من قبل أطراف مستقلة عن إدارة الأمن السيبراني مثل الإدارة المعنية بالمراجعة الداخلية أو طرف خارجي.

سياسة مراجعة وتدقيق الأمن السيبراني

بنود السياسة:

- يجب أن تتم مراجعة تطبيق ضوابط الأمن السيبراني للأنظمة الحساسة مرة واحدة كل ثلاث سنوات على الأقل من قبل أطراف مستقلة عن إدارة الأمن السيبراني من داخل الجهة.
- يجب التأكد من تطبيق ضوابط الأمن السيبراني دورياً، ومرّة واحدة سنوياً على الأقل للأنظمة الحسّاسة للتأكد من مواءمتها مع الضوابط الأساسية للأمن السيبراني (ECC:1-2018) وضوابط الأمن السيبراني للأنظمة الحساسة (CSCC-1:2019).
- يجب تحديد إجراءات مراجعة وتدقيق الأمن السيبراني وتوثيقها.
- يجب توثيق نتائج مراجعة وتدقيق الأمن السيبراني ومناقشتها مع الإدارات المعنية.
- يجب عرض النتائج على اللجنة الإشرافية للأمن السيبراني وصاحب الصلاحية، كما يجب أن تشمل النتائج نطاق المراجعة والتدقيق، والملاحظات المكتشفة، والتوصيات والإجراءات التصحيحية، وتقييم المخاطر وخطة معالجة الملاحظات.
- يجب اعتماد جدول المسؤوليات (RACI Chart) في تنفيذ عمليات مراجعة وتدقيق الأمن السيبراني.

سياسة الأمن السيبراني للموارد البشرية

تهدف هذه السياسة إلى توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة لضمان التأكد من أن مخاطر ومتطلبات الأمن السيبراني المتعلقة بالعاملين (موظفين ومتعاقدين) في الجهة تُعالج بفعالية قبل وأثناء وعند إنتهاء/إنهاء عملهم. كما تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة وأفضل الممارسات العالمية، وهي مطلب تشريعي في الضابط رقم ١-٩-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

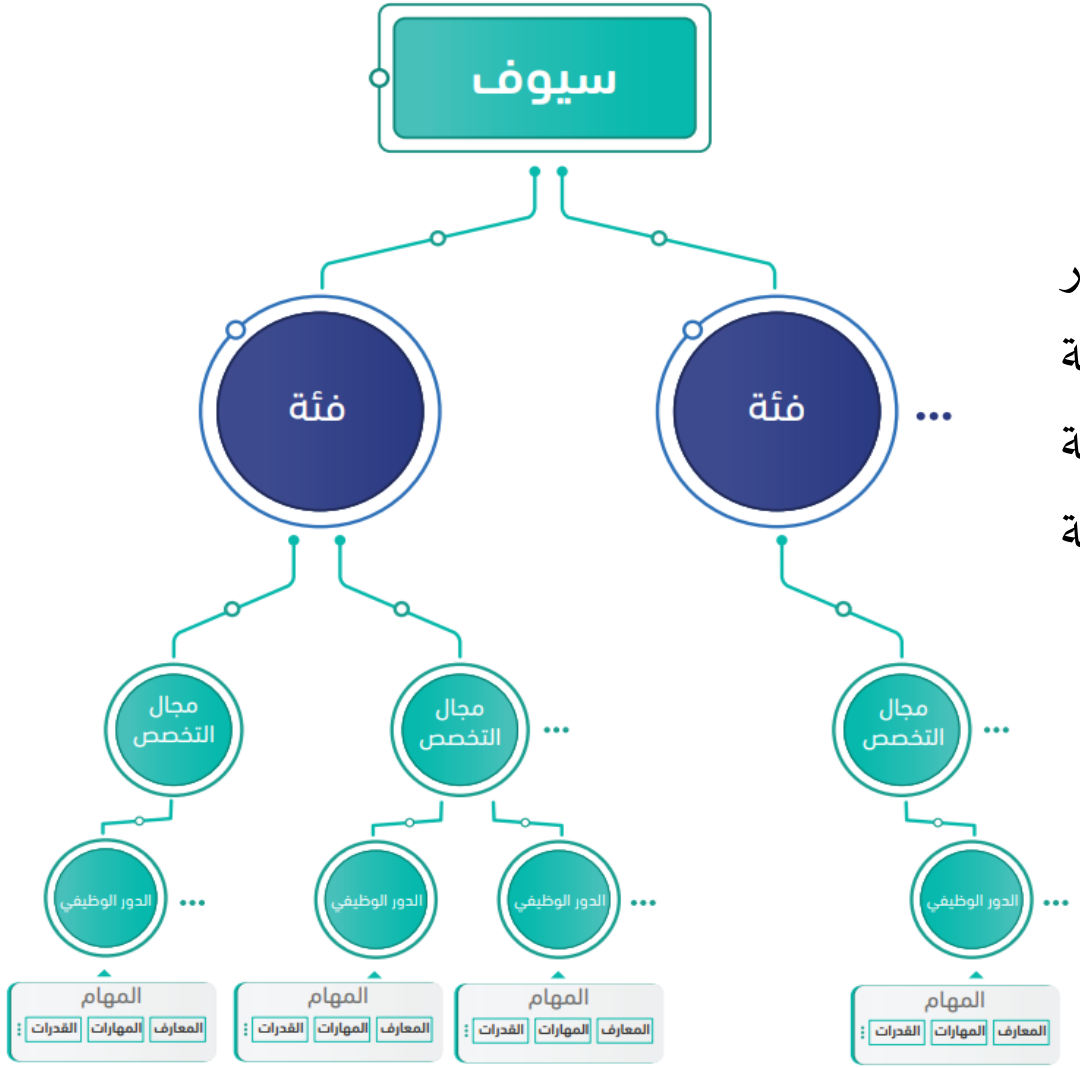
بنود السياسة:

- البنود العامة.
- بنود قبل التوظيف
- بنود أثناء العمل
- بنود إنتهاء الخدمة أو إنهاؤها

عصف ذهني

من وجهة نظرك
ما هي كوادر الأمن السيبراني
"سيوف"؟

الإطار السعودي لكوادر الأمن السيبراني (سيوف)



يهدف هذا الإطار لتأهيل الكوادر البشرية عند إتخاذ قرار تطبيق أي عمليات جديدة ضمن الأعمال فإن القوى البشرية تعتبر التحدي الأول لتطبيق هذا القرار، فوجود الكوادر المؤهلة والقادرة على فهم العمل بشكل جيد وتطبيقه بإحترافيه ودقة هو العامل الرئيسي الذي يدعم نجاح هذا القرار.

الإطار السعودي لكوادر الأمن السيبراني (سيوف)

يتضمن الإطار السعودي لكوادر الأمن السيبراني خمس فئات عمل واثنى عشر مجال تخصص وأربعين دوراً وظيفياً. ويتم تعريفها من خلال وصف موجز للأعمال التي يتم أداؤها في سياق الفئة المخصصة أو مجال التخصص أو الدور الوظيفي. ويرتبط كل دور وظيفي بمجموعة من المهام المطلوبة وقائمة بالمعارف والمهارات والقدرات اللازمة لأداء تلك المهام:

- **المعرفة**: هي مجموعة من البيانات والحقائق والمعلومات والنظريات والمفاهيم والقضايا والتوجهات ذات الصلة.
- **المهارة**: هي القدرة على تطبيق المعرفة وتسخير الأدوات والأساليب المناسبة لأداء مهمة معينة.
- **القدرة**: هي الكفاءة المستندة إلى السلوك التي يجب توفرها لأداء العمل في مجال معين.
- **المهمة**: هي مجموعة من الأنشطة التي يجب إكمالها كجزء من الدور الوظيفي.

شكراً لإستماعكم وتفاعلكم

- فترة الأسئلة -