دورة تدريبية: حوكمة الأمن السيبراني

# تطبيق ضوابط ومعايير الهيئة الوطنية للأمن السيبراني

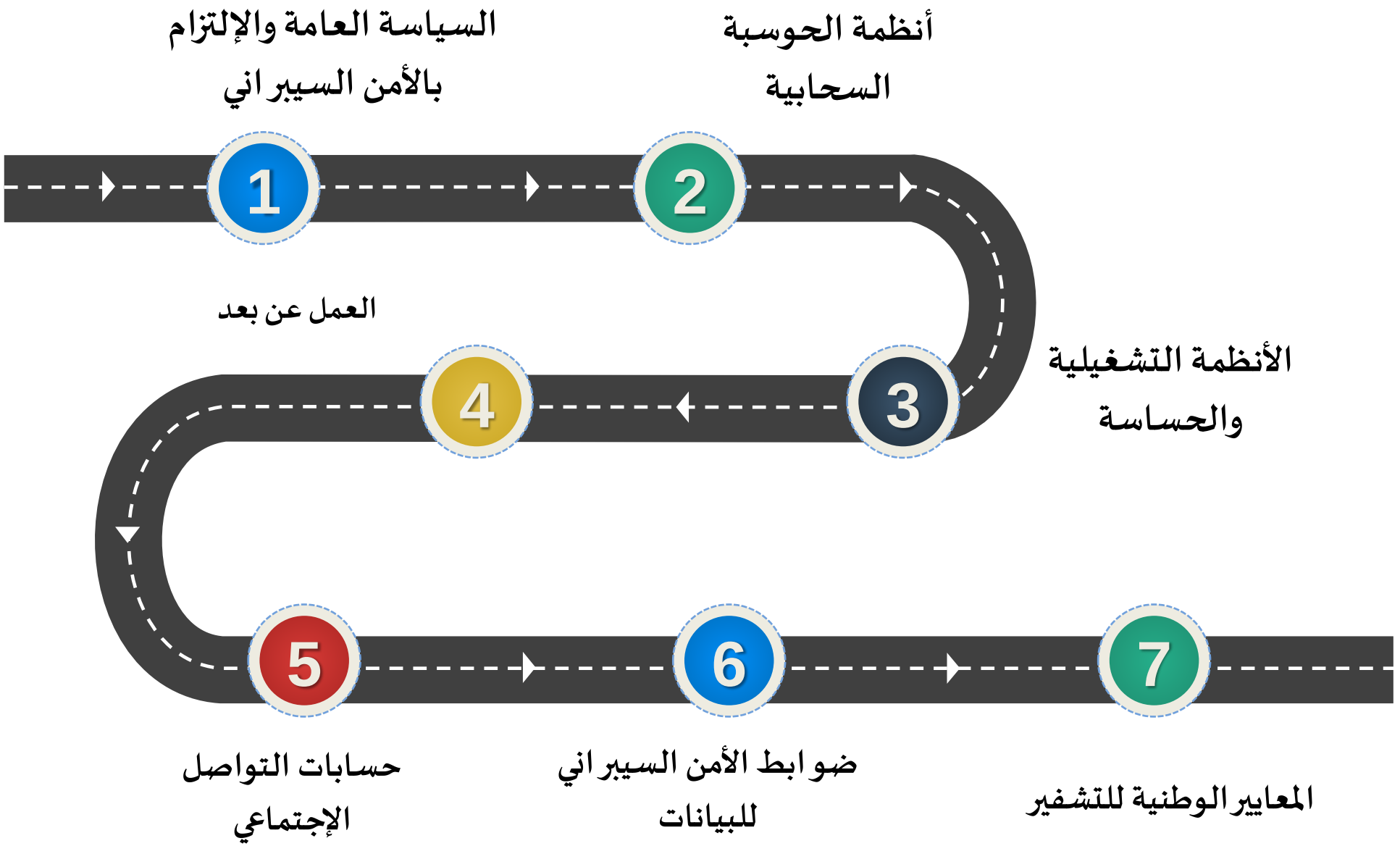
المحاضرة السابعة (الجزء الأول)

د. غالب الشمري

أستاذ الذكاء الإصطناعي وعلم البيانات المساعد

جامعة الملك سعود

# خارطة الطريق



# السياسة العامة للأمن السيبراني

الغرض الرئيسي من السياسة العامة للأمن السيبراني هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بتوثيق المتطلبات والتزام الجهة بها، لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية، ويتم ذلك من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها. وتهدف هذه السياسة إلى الالتزام بمتطلبات الأعمال التنظيمية الخاصة بالجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

## نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية للجهة، وتنطبق على جميع العاملين في الجهة. كما تعتبر هذه السياسة هي المحرك الرئيسي لجيمع سياسات الأمن السيبراني وإجراءاته ومعاييره ذات المواضيع المختلفة، وكذلك أحد المدخلات لعمليات الجهة الداخلية، مثل عمليات الموارد البشرية وعمليات إدارة الموردين وعمليات إدارة المشاريع وإدارة الغيير وغيرها.

عصف ذهني

من وجهة نظرك
ما هي عناصر السياسة العامة
لضوابط الأمن السيبراني؟


# عناصر السياسة العامة للأمن السيبراني

- يجب على إدارة الأمن السيراني تحديد معايير الأمن السيبراني وتوثيق سياساته وبرامجه، بناءً على نتائج تقييم المخاطر، وبشكل يضمن نشر متطلبات الأمن السيبراني، والتزام الجهة بها، وذلك وفقاً لمتطلبات الأعمال التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة، وإعتمادها من قبل رئيس الجهة. كما يجب إطلاع العاملين المعنيين في الجهةوالأطراف ذات العلاقة عليها.
- يجب على إدارة الأمن السيبراني تطوير سياسات الأمن السيبراني وبرامجه ومعاييره وتطبيقتها، والمتمثلة في:
  - برنامج إستراتيجية الأمن السيبراني: لضمان خطط العمل للأمن السيبراني والأهداف والمبادرات والمشاريع وفعاليتها داخل الجهة.
  - إدوار ومسؤوليات الأمن السيبراني: لضمان تحديد مهام ومسؤوليات واضحة لجميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني في الجهة.
  - برنامج إدارة المخاطر: لضمان إدارة المخاطر السيبرانية على نحو ممنهج يهدف لحماية الأصول المعلوماتية والتقنية في الجهة.
  - سياسة الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية: للتأكد من أن متطلبات الأمن السيبراني مضمنة في المشاريع.

# عناصر السياسة العامة للأمن السيبراني

- سياسة الإلتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني: للتأكد من برنامج الأمن السيبراني في الجهة متوافق مع المتطليات التشريعية والتنظيمية .
- سياسة المراجعة والتدقيق الدوري للأمن السيبراني: للتأكد من أن ضوابط الأمن السيبراني في الجهة مطبقة وتعمل وفقاً للسياسات والإجراءات التنظيمية للجهة والمتطلبات التشريعية الوطنية والدولية المقرة تنظيمياً.
- سياسة الأمن السيبراني المتعلقة بالموارد البشرية: للتأكد من أن مخاطر الأمن السيبراني ومتطلبات المتعلقة بالعاملين في الجهة تُعالج بفعالية قبل إنهاء عملهم، وأثنائه وعند إنتهائه وفقاً للسياسات والإجراءات للجهة.
- برنامج التوعية والتدريب بالأمن السيبراني: للتأكد من أن العاملين للجهة لديهم الوعي الأمني اللازم، وعلى دراية بمسؤولياتهم في مجال الأمن السيبراني، والتأكد بتزويد العاملين بالمهارات والمؤهلات والدروات التدريبية المناسبة.
- سياسة إدارة الأصول: للتأكد من أن الجهة لديها قائمة دقيقة وحديثة بالأصول المعلوماتية والتقنية المتوفرة في الجهة من أجل دعم العمليات التشغيلية للجهة ومتطلبات الأمن السيبراني.
- سياسة إدارة هويات الدخول والصلاحيات: لضمان حماية الأمن السيبراني للوصول المنطقي إلى الأصول المعلوماتية والتقنية للجهة من أجل منع الوصول غير المصرح به، وتقييد الوصول للأعمال المحددة في الجهة.

# عناصر السياسة العامة للأمن السيبراني

- سياسة حماية الأنظمة وأجهزة معالجة المعلومات: لضمان حماية الأنظمة وأجهزة معالجة المعلومات، بما في ذلك أجهزة المستخدمين والبنى التحتية في الجهة من المخاطر السيبرانية.
- سياسة حماية البريد الإلكتروني: لضمان حماية البريد الإلكتروني للجهة من المخاطر السيبرانية.
- سياسة إدارة أمن الشبكات: لضمان حميات شبكات الجهة من المخاطر السيبرانية.
- سياسة أمن الأجهزة المحمولة: لضمان حماية أجهزة الجهة المحمولة (أجهزة الحاسب المحمولة، الهواتف الذكية، الأجهزة اللوحية) من المخاطر السيبرانية ولضمان التعامل بشكل آمن مع المعلومات الحساسة والخاصة بأعمال الجهة.
- سياسة حماية البيانات والمعلومات: لضمان حماية السرية، وسلامة بيانات ومعلومات الجهة ودقتها وتوافرها.
- سياسة التشفير ومعياره: لضمان الإستخدام السليم والفعال للتشفير، لحماية الأصول المعلوماتية الإلكترونية للجهة وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة.
- سياسة إدارة النسخ الإحتياطية: لضمان حماية بيانات الجهة ومعلوماتها، وكذلك حماية الإعدادات التقنية للأنظمة والتطبيقات الخاصة بالجهة من الأضرار الناجمة عن المخاطر السيبرانية.

# عناصر السياسة العامة للأمن السيبراني

- سياسة إدارة الثغرات ومعياره: لضمان إكتشاف الثغرات التقنية في الوقت المناسب، ومعالجتها بشكل فعال وذلك لمنع إحتمالية إستغلال هذه الثغرات من قبل الهجمات السيبرانية، وتقليل الآثار المترتبة على أعمال الجهة.
- سياسة إختبار الإختراق ومعياره: لتقييم مدى فعالية قدرات تعزيز الأمن السيبراني وإختباره في الجهة وذلك من خلال محاكاة تقنيات الهجوم السيبراني الفعلية واساليبه، لإكتشاف نقاط الضعف الأمنية الغير معروفة والتي تؤدي إلى إختراق الجهة.
- سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني: لضمان جمع سجلات أحداث الأمن السيبراني، وتحليلها، ومراقبتها في الوقت المناسب، من أجل الإكتشاف الإستباقي للهجمات السيبرانية، وإدارة مخاطرها بفعالية لمنع الآثار السلبية المحتملة على أعمال الجهة..
- سياسة إدارة حوادث وتهديدات الأمن السيبراني: لضمان إكتشاف حوادث الأمن السيبراني وتحديدها في الوقت المناسب وإدارتها بشكل فعال، والتعامل مع التهديدات السيبرانية ومنع الآثار السلبية المحتملة على أعمال الجهة مع مراعاة ما ورد بالأمر السامي رقم 37140.
- سياسة الأمن المادي: لضمان حماية الأصول المعلوماتي والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب.
- سياسة حماية تطبيقات الويب ومعياره: لضمان حماية تطبيقات الويب الداخلية والخارجية للجهة من المخاطر السيبرانية.

# عناصر السياسة العامة للأمن السيبراني

- جوانب صمود الأمن السيبراني في إدارة إستمرارية الأعمال: لضمان توافر متطلبات صمود الأمن السيبراني في إستمرارية أعمال الجهة، ولضمان معالجة الآثار المرتبة على الإضطرابات في الخدمات الإلكترونية الحرجة وتقليلها على الجهة.
- سياسة الأمن السيبراني المتعلقة بالأطراف الخارجيةلضمان حماية أصول الجهة من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية، بما في ذلك خدمات الإسناد والخدمات المدراة وفقاً للسياسات والإجراءات التنظيمية للجهة.
- سياسة الأمن السيبراني المتعلقة بالحوسبة الحسابية والإستضافة: لضمان معالجة المخاطر السيبرانية وتنفيذ متطلبات الأمن السيبراني للحوسبة السحابية والإستضافة بشكل ملائم وفعال ووفقاً للسياسات والإجراءات التنظيمية للجهة.
- سياسة حماية الأجهزة وأنظمة التحكم الصناعي: لضمان إدارة الأمن السيبراني بشكل سليم وفعال، لحماية توافر أصول الجهة وسلامتها وسريتها، وهي الأصول المتعلقة بأنظمة التحكم الصناعي ضد الهجوم السيبراني، مثل: الوصول الغير مصرح به، التخريب، التجسس، والتلاعب بما يتناسق مع إستراتيجية الأمن السيبراني للجهة.

- يحق لإدارة الأمن السيبراني الإطلاع على المعلومات، وجمع الأدلة اللازمة، للتأكد من الإلتزام بالمتطلبات التشريعية والتنظيمية ذات العلاقة المتعلقة بالأمن السيبراني

# الأدوار والمسؤوليات

تُمثل القائمة التالية مجموعة من الأدوار والمسؤوليات اللازمة لإقرار سياسات الأمن السيبراني وإجراءاته، ومعاييره وبرامجه، وتنفيذها وإتباعها:

- مسؤوليات صاحب الصلاحية "رئيس الجهة"، على سبيل المثال: إنشاء لجنة إشرافية للأمن السيبراني ويكون "رئيس إدارة الأمن السيبراني" أحد أعضائها.
- مسؤوليات "إدارة الشؤون القانونية"، على سبيل المثال: التأكد من أن معايير الأمن السيبراني والمحافظة على سرية المعلومات، ومَلزمة قانونياً في عقود العاملين في الجهة والأطراف الخارجية.
- مسؤوليات "إدارة التدقيق والمراجعة الداخلية"، على سبيل المثال: مراجعة ضوابط الأمن السيبراني وتدقيق تطبيقها.
- مسؤوليات "إدارة الموارد البشرية"، على سبيل المثال: تطبيق متطلبات الأمن السيبراني المتعلقة بالعاملين في الجهة.
- مسؤوليات "إدارة الأمن السيبراني"، على سبيل المثال: الحصول على موافقة رئيس الجهة على سياسات الأمن السيبراني.
- مسؤوليات "رؤساء الإدارات"، لدعم سياسات الأمن السيبراني وإجراءاته ومعايير وبرامجه، وتوفير جميع الموارد اللازمة.
- مسؤوليات "العاملين"، على سبيل المثال: لمعرفة متطلبات الأمن السيبراني المتعلقة بالعاملين في الجهة والإلتزام بها.

# الإلتزام بالسياسة

- يجب على صاحب الصلاحية (رئيس الجهة) ضمان الإلتزام بسياسة الأمن السيبراني ومعاييره.
- يجب على "رئيس إدارة الأمن السيبراني" للتأكد من إلتزام الجهة بسياسات الأمن السيبراني ومعاييره بشكل دوري.
- يجب على جميع العاملين في الجهة الإلتزام بهذه السياسة.
- قد يُعرض إي إنتهاك للسياسات المتعلقة بالأمن السيبراني صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في الجهة.

# الإستثناءات

يُمنع تجاوز سياسات الأمن السيبراني ومعاييره، دون الحصول على تصريح رسمي مسبق من رئيس إدارة الأمن السيبراني أو اللجنة الإشرافية للأمن السيبراني، ما لم يتعارض مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

# سياسة الإلتزام بتشريعات وتنظيمات الأمن السيبراني

الغرض الرئيسي من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لضمان التأكد من أن برنامج الأمن السيبراني لدى الجهة يتوافق مع المتطلبات التشريعية والتنظيمية. وتهدف إلى الإلتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية، وهي مطلب تشريعي في الضابط رقم 1-7-1 من الضوابط الأساسية للأمن السيبراني.

## نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأنظمة، والإجراءات الخاصة باللجنة وتنطبق على جميع العاملين في الجهة.

## الأدوار والمسؤوليات:

- راعي ومالك وثيقة السياسة: رئيس إدارة الأمن السيبراني
- مراجعة السياسة وتحديثها: إدارة الأمن السيبراني
- تنفيذ الساسية وتطبيقها: إدارة الأمن السيبراني

# سياسة الإلتزام بتشريعات وتنظيمات الأمن السيبراني

## بنود سياسة التشريعات والتنظيمات

- يجب تحديد قائمة التشريعات والتنظيمات المتعلقة بالأمن السيبراني، والمتطلبات وتحديثها دورياً.
- يجب توفير التقنيات اللازمة للتحقق من الإلتزام بمتطلبات الجهة التشريعية والتنظيمية.
- يجب مراجعة سياسات الأمن السيبراني وإجراءاته دورياً لضمان الإلتزام التشريعي والتنظيمي للجهة.
- يجب التأكد من تطبيق سياسات الأمن السيبراني وإجراءاته دورياً.
- يجب التأكد من الإلتزام بالمتطلبات التشريعية والتنظيمية بشكل دوري عن طريق الأدوات المناسبة مثل:
  - أنشطة تقييم الأمن السيبراني
  - أنشطة إدارة الثغرات
  - أنشطة إختبار الإختراقات
  - مراجعة معايير الأمن السيبراني
  - المراجعة الأمنية للشفرة المصدرية
  - إستبيانات المستخدمين
  - المقابلات مع أصحاب المصلحة
  - مراجعة الصلاحياتعلى النظام والشبكة
  - مراجعة سجلات الأمن السيبراني وحوادثه

# سياسة الإلتزام بتشريعات وتنظيمات الأمن السيبراني

## بنود سياسة التشريعات والتنظيمات

- يجب تحديد الإجراءات التصحيحية اللازمة والعمل على تطبيقها، لتصحيح الثغرات لجميع متطلبات الإلتزام من قبل أصحاب العلاقة.
- يجب إستخدام مؤشر قياس الأداء KPI لضمان التطوير المستمر لبرامج الإلتزام
- يجب تنفيذ الإجراءات المناسبة، لضمان الإلتزم بالمتطلبات التشريعية والتنظيمية المتعلقة بحقوق الملكية الفكرية، وإستخدام البرمجيات.

## الإلتزام بالسياسة

- يجب على رئيس إدارة الأمن السيبراني ضمان إلتزام الجهة بهذه السياسة بشكل دوري.
- يجب على جميع العاملين بالجهة الإلتزام بهذه السياسة.
- قد يعرض أي إنتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الأنظمة المتبعة في الجهة

عصف ذهني

من وجهة نظرك
ما هي ضوابط الأمن السيبراني
للحوسبة السحابية؟


# ضوابط الأمن السيبراني للحوسبة السحابية

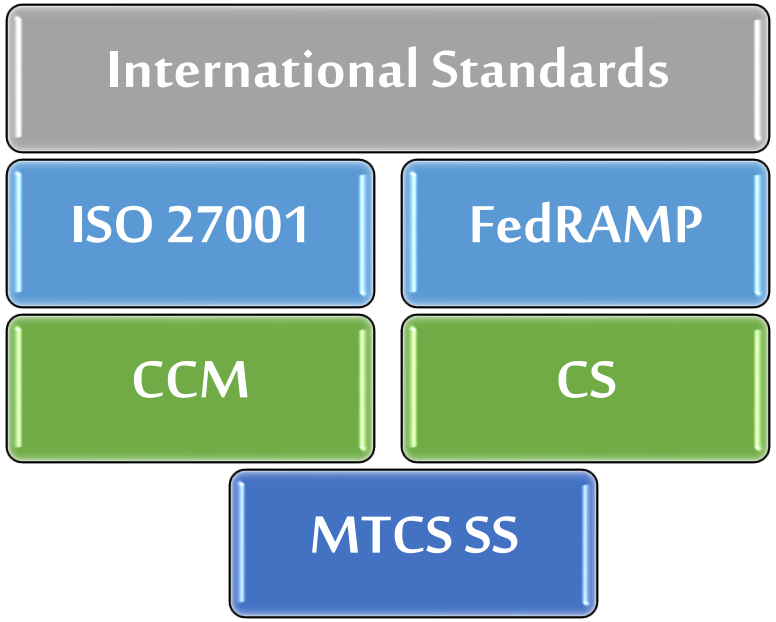
## مكونات ضوابط الأمن السيبراني للحوسبة السحابية

تتألف ضوابط الأمن السيبراني للحوسبة السحابية من المكونات التالية:

| لمقدمي الخدمات | للمشتركين |
|---|---|
| ٤ مكونات أساسية<br>(4 Main Domains) | |
| ٢٤ مكونًا فرعيًا<br>(24 Subdomains) | |
| ٣٧ ضابطًا أساسيًا<br>(37 Main Controls) | ١٨ ضابطًا أساسيًا<br>(18 Main Controls) |
| ٩٦ ضابطًا فرعيًا<br>(96 Subcontrols) | ٢٦ ضابطًا فرعيًا<br>(26 Subcontrols) |

# منهجية ضوابط الأمن السيبراني للحوسبة السحابية

في سبيل تحقيق أهداف ضوابط الأمن السيبراني للحوسبة السحابية، فقد تبنت منهجية التصميم المتبعة مراجعة التشريعات المتعلقة بالحوسبة السحابية وإستناداً إلى هذه المراجع، طورت الهيئة ضوابط الأمن السيبراني للحوسبة السحابية لتكون إمتداداً مكملاً للضوابط الأساسية للأمن السيبراني من حيث العمق والشمول في قطاع الحوسبة السحابية. وخلال تطوير ضوابط الأمن السيبراني للحوسبة السحابية، تم إعداد قائمة موحدة من المتطلبات الأمنية في المجالات ذات الصلة من **خمسة معايير مرجعية في مجال الأمن السيبراني للحوسبة السحابية** لتشكيل مجموعة مدمجة من ضوابط الحوسبة السحابية.



عصف ذهني

من وجهة نظرك
ما هي ضوابط الأمن السيبراني
للأنظمة التشغيلية والحساسة؟


# ضوابط الأمن السيبراني للأنظمة التشغيلية والحساسة

قامت الهيئة بإصدار ضوابط خاصة بالأنظمة التشغيلية بعد دراسة عدة معايير وأطر وضوابط للأمن السيبراني، تم إعدادها من قبل منظمات وجهات محلية ودولية للإطلاع على أفضل الممارسات والتجارب ذات العلاقة في مجال الأمن السيبراني للأنظمة التشغيلية وعمل مواءمة مع عدد من الضوابط والمعايير الدولية.

تتكون ضوابط الأمن السيبراني للأنظمة التشغيلية، من:

- 4 مكونات أساسية
- 23 مكوناً فرعياً
- 47 ضابطاً أساسياً
- 122 ضابطاً فرعياً

# ضوابط الأمن السيبراني للأنظمة التشغيلية والحساسة

قامت الهيئة بإصدار ضوابط خاصة بالأنظمة الحساسة بعد دراسة عدة معايير وأطر وضوابط للأمن السيبراني، تم إعدادها من قبل منظمات وجهات محلية ودولية للإطلاع على أفضل الممارسات والتجارب ذات العلاقة في مجال الأمن السيبراني للأنظمة الحساسة وعمل مواءمة مع عدد من الضوابط والمعايير الدولية.

الأنظمة الحساسة: هي أي أنظمة أو شبكات يؤدي تعطلها أو التغيير الغير مشروع لطريقة عملها أو الدخول الغير مصرح به لها، أو للبيانات والمعلومات التي تحفظها أو تعالجها، إلى التأثير السلبي على توافر الخدمات أو أعمال الجهة العامة، أو إحداث آثار إقتصادية أو مالية أو أمنية، أو إجتماعية سلبية كبيرة على المستوى الوطني.

تتكون ضوابط الأمن السيبراني للأنظمة الحساسة، من:

- 4 مكونات أساسية
- 21 مكوناً فرعياً
- 32 ضابطاً أساسياً
- 73 ضابطاً فرعياً

Critical Systems Cybersecurity controls.pdf

عصف ذهني

من وجهة نظرك
ما هي ضوابط الأمن السيبراني
للعمل عن بعد؟


# ضوابط الأمن السيبراني للعمل عن بعد

قامت الهيئة بإصدار ضوابط خاصة بالعمل عن بعد ودراسة عدة معايير وأطر وضوابط للأمن السيبراني، تم إعدادها من قبل منظمات وجهات محلية ودولية للإطلاع على أفضل الممارسات والتجارب ذات العلاقة في مجال الأمن السيبراني للعمل عن بعد وعمل مواءمة مع عدد من الضوابط والمعايير الدولية.

تتكون ضوابط الأمن السيبراني العمل عن بعد، من:

- 3 مكونات أساسية
- 16 مكوناً فرعياً
- 21 ضابطاً أساسياً
- 42 ضابطاً فرعياً

عصف ذهني

من وجهة نظرك
ما هي ضوابط الأمن السيبراني
لحساب التواصل الإجتماعي؟


# ضوابط الأمن السيبراني لحسابات التواصل الإجتماعي

قامت الهيئة بإصدار ضوابط خاصة لحسابات التواصل الاجتماعي ودراسة عدة معايير وأطر وضوابط للأمن السيبراني، تم إعدادها من قبل منظمات وجهات محلية ودولية للإطلاع على أفضل الممارسات والتجارب ذات العلاقة في مجال الأمن السيبراني لحسابات التواصل الاجتماعي وعمل مواءمة مع عدد من الضوابط والمعايير الدولية.

تتكون ضوابط الأمن السيبراني لحسابات التواصل الإجتماعي، من:

- 3 مكونات أساسية
- 12 مكوناً فرعياً
- 15 ضابطاً أساسياً
- 38 ضابطاً فرعياً

عصف ذهني

من وجهة نظرك
ما هي ضوابط الأمن السيبراني
للبيانات؟

# ضوابط الأمن السيبراني للبيانات

قامت الهيئة بإصدار ضوابط خاصة للبيانات ودراسة عدة معايير وأطر وضوابط للأمن السيبراني، تم إعدادها من قبل منظمات وجهات محلية ودولية للإطلاع على أفضل الممارسات والتجارب ذات العلاقة في مجال الأمن السيبراني للبيانات وعمل مواءمة مع عدد من الضوابط والمعايير الدولية.

تتكون ضوابط الأمن السيبراني للبيانات، من:

- 3 مكونات أساسية
- 11 مكوناً فرعياً
- 19 ضابطاً أساسياً
- 47 ضابطاً فرعياً

عصف ذهني

من وجهة نظرك
ما هي ضوابط الأمن السيبراني
للمعايير الوطنية للتشفير؟


# ضوابط الأمن السيبراني للمعايير الوطنية للتشفير

قامت الهيئة بإصدار ضوابط خاصة للمعايير الوطنية للتشفير ودراسة عدة معايير وأطر وضوابط للأمن السيبراني، تم إعدادها من قبل منظمات وجهات محلية ودولية للإطلاع على أفضل الممارسات والتجارب ذات العلاقة في مجال الأمن السيبراني للمعايير الوطنية للتشفير وعمل مواءمة مع عدد من الضوابط والمعايير الدولية.

هذه الوثيقة التي تطلق عليها المعايير الوطنية للتشفير NCS-1: 2020 تحدد الحد الأدنى من متطلبات التشفير للأغراض المدنية والتجارية وذلك لحماية البيانات عند تخزينها، أو معالجتها أو نقلها، والأنظمة والشبكات الوطنية.

التشفير هو عبارة عن ممارسة حماية البيانات بإستخدام الخوارزميات المشفرة وذلك من خلال تحويل تنسيق البيانات القابلة للقراءة إلى تنسيق مشفر لا يمكن قراءة البيانات أو معالجتها الإ بعد فك تشفيرها.

National Cryptographic Standards.pdf

شكراً لإستماعكم وتفاعلكم

- فترة الأسئلة -