دليل الالتزام بضوابط ومتطلبات الأمن السيبراني في المملكة العربية السعودية

دليل مبدئي للامتثال للوائح الأمن
السيبراني الوطنية في المملكة

لمحة عامة عن الدليل

خلال الأعوام القليلة الماضية، جرى اعتماد مجموعة من اللوائح التي تُعنى بالأمن السيبراني في المملكة العربية السعودية، الأمر الذي أثّر بشكل ملحوظ في المنظمات الحكومية والبنية التحتية الوطنية الحساسة في المملكة، ودفع بالعديد من هذه الجهات إلى إعداد برامج خاصة بالأمن السيبراني لاستيفاء متطلبات هذه اللوائح

لقد قمنا بإعداد هذا الدليل الذي يتناول مسألة الالتزام بمتطلبات وضوابط الأمن السيبراني في المملكة لتبسيط المتطلبات ومساعدتكم على الانطلاق في رحلة التزامكم بالأمن السيبراني

الخطوات الرئيسية لبرنامج فعال للأمن السيبراني

مقدّمة إلى مكوّنات الأمن السيبراني والإجراءات الرئيسية

بهدف الالتزام باللوائح الوطنية للأمن السيبراني في المملكة، لا بدّ من اتخاذ عدد من الإجراءات الرئيسية التي تنضوي تحت مظلة الحوكمة، والأشخاص، والتقنية

الإجراءات المرتبطة بالحوكمة التي تركّز على الإدارة التنظيمية وتقوم بضبط تدابير التطبيق اللازمة للالتزام بمتطلبات وضوابط الأمن السيبراني

الإجراءات المرتبطة بالأشخاص التي تركّز على تدابير الأمن السيبراني التي يجب اتخاذها على مستوى الموارد البشرية ورأس المال البشري

الإجراءات المرتبطة بالتقنية التي تركّز على الحلول، والأدوات، والآليات التقنية التي يجب تنفيذها بهدف الالتزام بمتطلبات وضوابط الأمن السيبراني

يتمّ اتخاذ هذه الإجراءات على مستوى العديد من المكوّنات الرئيسية والمكوّنات الفرعية المتوائمة مع اللوائح الوطنية للأمن السيبراني التي تعتمدها المملكة

حوكمة الأمن السيبراني

هي العملية التي تقضي بوضع تدابير تنظيمية تحرص على مواءمة البرنامج الأمني للجهة مع أهداف الأعمال، والالتزام باللوائح المعمول بها، وتحقيق الأهداف التي تُعنى بإدارة مخاطر الأمن السيبراني

تعزيز الأمن السيبراني

يقوم على الخطوات المنسقة للمقاومة والدفاع عن المعلومات، والنظم، والشبكات من الهجمات السيبرانية من خلال تنفيذ عمليات وآليات الحماية لتحديد الحوادث التي تطرأ ضمن الشبكات، وتحليلها، والاستجابة لها، والإبلاغ عنها

صمود الأمن السيبراني

هو القدرة على التوقّع، والصمود، والتعافي، والتكيّف مع الظروف المعاكسة، أو الضغوط، أو الهجمات، أو الانتهاكات الأمنية التي تطال الأصول المعلوماتية والتقنية

الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية

هو العملية التي تقضي بتطبيق تدابير الأمن السيبراني لضمان الإدارة، والمراقبة، والمعالجة الفعالة للمخاطر التي تنشأ نتيجة التعاملات والاتفاقيات مع الأطراف الخارجية ومقدّمي الخدمة

الأمن السيبراني لأنظمة التحكم الصناعي

هو القدرة على الدفاع عن أنظمة التحكم الصناعي والتقنيات التشغيلية من خلال تنفيذ عمليات وآليات أمنية لحمايتها

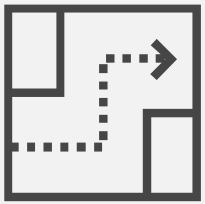
الخطوات الرئيسية لبرنامج فعال للأمن السيبراني

01

مواءمة أهداف الأمن السيبراني مع احتياجات الجهات

02

تحديد توجّه استراتيجي لجهود الأمن السيبراني



03

إنشاء إدارة للأمن السيبراني وتشكيل فريق عمل

04

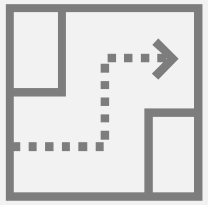
تعزيز سياسة الأمن السيبراني على نطاق الجهة ككل

05

بناء القدرات في مجال الأمن السيبراني

01
مواءمة أهداف الأمن السيبراني مع احتياجات الجهات

02
تحديد توجّه استراتيجي لجهود الأمن السيبراني



وضعت الجهات الحكومية في المملكة مجموعة من الأهداف الاستراتيجية والتكتيكية سعيًا لتحقيق أهداف رؤية ٢٠٣٠ التي أطلقتها المملكة، ويشمل ذلك التحوّل الرقمي للعديد من القطاعات الرئيسية. وأصدرت الهيئة الوطنية للأمن السيبراني في المملكة العديد من اللوائح المتعلّقة بالأمن السيبراني التي يتعيّن على جميع الجهات الحكومية والبنية التحتية الوطنية الحساسة الالتزام بها. وعليه، بات الأمن السيبراني من بين مهام الأعمال الرئيسية لجميع الجهات الحكومية والبنية التحتية الوطنية الحساسة

إن مشهد الالتزام بلوائح الأمن السيبراني معقد، وهو يخضع لسلسلة من التغييرات باستمرار. ويعرض هذا المشهد العديد من التحديات التي تواجهها الجهات نتيجة التكاليف الإضافية وغياب اليقين على مستويات عديدة حول كيفية الالتزام بمتطلبات وضوابط الأمن السيبراني

يجب أن تكون جميع الخطوات والإجراءات لإعداد برنامج فعال للأمن السيبراني متوائمة مع احتياجات المنظمة والأعمال، ويشمل ذلك

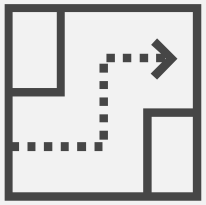
- فهم مهام الأعمال التي ستساعد في تحديد نطاق برنامج الأمن السيبراني في المنظمة
- فهم التوجّه الاستراتيجي للمنظمة، ما من شأنه أن يساعد في تحديد التوجّه الاستراتيجي للأمن السيبراني (يُرجى مراجعة الخطوة ٢). ومن الممكن أن تتخذ العلاقة والمواءمة بين الأعمال والأمن السيبراني أشكالًا عديدة على النحو المبيّن في الجدول أدناه

	الأمن السيبراني تفاعلي (بعد الحدث)	برنامج الأمن السيبراني متوائم مع احتياجات وأهداف الأعمال		
العلاقة بين الجهة والأمن السيبراني	**العرقلة**	**الدعم**	**التمكين**	**القيادة**
الوصف	يُعتبر الأمن السيبراني من بين الأفكار التي تطرأ في مرحلة لاحقة أو متأخرة، ويعيق تحقيق أهداف الأعمال. وترى الجهة بأن الأمن السيبراني دائما يؤدي إلى عرقلة أنشطتها	يستطيع الأمن السيبراني تحديد الفرص التي تدعم أهداف الأعمال تعديل احتياجاتهم والاستجابة لها.	يستطيع الأمن السيبراني تحديد الفرص التي تساهم في التمكين لتحقيق أهداف الأعمال. ويقدّم الأمن السيبراني حلولًا لتلبية احتياجات الأعمال.	يستطيع الأمن السيبراني تحديد الفرص التي تساهم في تحقيق أهداف الأعمال. ويقدّم الأمن السيبراني، وبصورة استباقية، حلولًا تساعد في رسم معالم أهداف الأعمال.
المثال #1	رفض جميع الحلول السحابية	تقييد الحلول السحابية وطلب تبريرات الأعمال	تضمين الحلول السحابية من خلال إطار وبنية الأمن السحابيين	تقديم الحلول الأمنية السحابية لتعزيز وضع الأمن السيبراني
المثال #2	منع الوصول إلى جميع وسائط التخزين الخارجية مثل محرك أقراص فلاش (USB)	تقييد الوصول إلى وسائط التخزين الخارجية وطلب تبرير من الأعمال	تقديم الأكشاك الأمنية لوسائط التخزين الخارجية	تقديم الآليات المؤتمتة لمشاركة المعلومات بشكل آمن

مواءمة أهداف
الأمن السيبراني
مع احتياجات
احتياجات الجهات

02

تحديد توجّه
استراتيجي لجهود
الأمن السيبراني



03

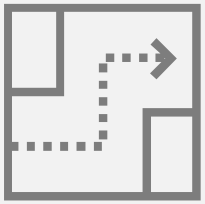
إنشاء إدا
السيبراني
فريق عم

ستشعر المنظمة بضرورة السعي إلى تحقيق أهدافها بعد إقرار وإصدار استراتيجية شاملة للأمن السيبراني تتضمّن رؤية المنظمة، ورسالتها وأهدافها. وتشكّل رؤية المنظمة ورسالتها الحافز الذي يشجع على تطوير استراتيجية تؤدي إلى إحداث تغييرات

وعليه، ومن أجل وضع خطة للأمن السيبراني قابلة للتنفيذ، يتعيّن على المنظمة أولًا فهم وضعها الراهن في ما يخص الأمن السيبراني. ويمكن فهم هذا الوضع من وجهات نظر مختلفة بدءًا من مستوى النضج الحالي للأمن السيبراني، والمخاطر الحالية التي تهدد الأمن السيبراني، وصولًا إلى الثغرات التقنية. ولا بدّ للخطة القابلة للتنفيذ من تحديد الإجراءات على النحو المبيّن في الأقسام التالية (من القسم ٣ إلى القسم ٦) من أجل تفصيل تنفيذ الأهداف الاستراتيجية للمنظمة

02

تحديد توجّه استراتيجي لجهود الأمن السيبراني



03

إنشاء إدارة للأمن السيبراني وتشكيل فريق عمل

04

تعزيز سيا
السيبراني ع
الجهة ككل

إنشاء قسم مخصص للأمن السيبراني يتمتّع بالخصائص التالية

- يكون مستقلًا عن أقسام وإدارات تقنية المعلومات
- يرتبط مباشرةً برئيس المنظمة أو نائبه
- يرأسه مواطن متفرغ ذو كفاءة عالية في مجال الأمن السيبراني

إنشاء لجنة توجيهية مستقلة للأمن السيبراني أو إدراج مهام لجنة للأمن السيبراني ضمن مهام إحدى اللجان القائمة (مثل لجنة الحوكمة والمخاطر والالتزام التابعة للمنظمة) التي ترتبط مباشرةً برئيس المنظمة. ومن شأن ذلك أن يضمن توفير الدعم القيادي في تنفيذ متطلبات الأمن السيبراني في مختلف أقسام المنظمة

05

بناء القدرات في
مجال الأمن السيبراني

04

تعزيز سياسة الأمن
السيبراني على نطاق
الجهة ككل

من المهم جدًا بالنسبة إلى أيّ منظمة أن تضع سياسة شاملة للأمن السيبراني تتطرّق إلى التحديات المرتبطة بالتهديدات المتغيّرة باستمرار ومتطلبات الالتزام المعقدة. ستضمن سياسة الأمن السيبراني قدرة المنظمة على تنسيق وتطبيق برنامج للأمن السيبراني على مستوى المنظمة ككل، من شأنه أن يساهم في الترويج لمتطلبات الأمن السيبراني وإبلاغ إدارات المنظمة كافة على الصعيد الداخلي، والأطراف الخارجية، والمورّدين، ومقدّمي الخدمة التابعين بها على الصعيد الخارجي بهذه المتطلبات

ولكي تكون هذه السياسة فعالة، يتعيّن على المنظمة أولًا تحديد ضوابط الأمن السيبراني ذات الصلة واللازمة لحماية أعمالها، وعملياتها التشغيلية، والأشخاص التابعين لها. ويجب أن يشمل ذلك المتطلبات العامة ضمن سياسة الأمن السيبراني، إلى جانب المعايير التقنية، والإجراءات، والأطر، والإرشادات. علاوةً على ذلك، ينبغي توثيق متطلبات الأمن السيبراني، واعتمادها، والإبلاغ بها، ومراجعتها على نحو منتظم وذلك وفقًا للفترات الزمنية المخطط لها أو عندما يتطلّب قسم الأمن السيبراني إجراء تغييرات. في الواقع، يضطلع قسم الأمن .السيبراني بدور مهم في الحرص على الإبلاغ بمتطلبات الأمن السيبراني، وتنفيذها، ومراجعتها ضمن المنظمة

05

بناء القدرات في مجال الأمن السيبراني

يحدّد هذا الدليل الجوانب المتعلّقة بالتوثيق، والتقنية، والأشخاص لقدرات الأمن السيبراني التسع عشرة التي يتعيّن على كل منظمة تنفيذها لحماية معلوماتها وأصولها والالتزام بلوائح الأمن السيبراني

04

تعزيز سياسة الأمن سيبراني على نطاق جهة ككل

التخطيط لمتطلبات المخاطر والالتزام	تضمين المتطلبات الأمنية في العمليات المعنية بالموارد البشرية	تعزيز ثقافة الوعي بالأمن السيبراني
حوكمة الهويات وإدارة صلاحيات الدخول	معرفة وحماية البيانات	حماية نظم تقنية المعلومات
حماية التواصل الإلكتروني	تطوير وصيانة التطبيقات الآمنة	حماية الأجهزة المحمولة
حماية الشبكات	الدفاع عن التقنية التشغيلية	حماية الأجهزة والأصول
إدارة الثغرات ونقاط الضعف	تحديد حالات الانكشاف المحتملة بواسطة اختبار الاختراق	مراقبة واكتشاف تهديدات الأمن السيبراني
تعزيز عمليات الأمن السيبراني والمعلومات الاستباقية	الاستجابة لحوادث الأمن السيبراني	تطوير خطط التعافي وضمان استمرارية الخدمات
إدارة وحماية الأمن السيبراني المتعلّق بالحوسبة السحابية والاستضافة	تضمين متطلبات السيبراني في الاتفاقيات مع الأطراف الخارجية	

التخطيط لمتطلبات المخاطر والالتزام

التوثيق

- وضع سياسة للأمن السيبراني تتضمّن متطلبات إدارة مخاطر الأمن السيبراني، بما يشمل إعداد منهجية وعملية إدارة مخاطر الأمن السيبراني، إلى جانب تحديد المحرّكات لتقييم مخاطر الأمن السيبراني
- وضع سياسة للأمن السيبراني تتضمّن متطلبات الالتزام بلوائح الأمن السيبراني، بما يشمل تحديد اللوائح والتنظيمات الوطنية والدولية للأمن السيبراني التي يتعيّن على المنظمة الالتزام بها
- إعداد خطة لإجراء عمليات المراجعة الذاتية والتدقيق الدوري للأمن السيبراني لدى المنظمة لتقييم مدى الالتزام بسياسات الأمن السيبراني والمتطلبات التنظيمية
- إعداد خطة لإجراء عمليات المراجعة والتدقيق السنوية من قبل أطراف مستقلة عن قسم الأمن السيبراني لتقييم مدى الالتزام بسياسات الأمن السيبراني والمتطلبات التشريعية والتنظيمية

التقنية

- تطبيق أداة للحوكمة، والمخاطر، والالتزام لتمكين منظمتكم من تنفيذ ودمج عمليات الحوكمة، وإدارة المخاطر، والالتزام بشكل فعال

المسؤوليات

- تتولى الإدارة المعنية بالأمن السيبراني إجراء عمليات تقييم مخاطر الأمن السيبراني، ومراقبة تنفيذ خطط مواجهة هذه المخاطر والتعامل معها داخل المنظمة

تضمين المتطلبات الأمنية في العمليات المعنية بالموارد البشرية

التوثيق

- وضع سياسة للأمن السيبراني تتضمّن المتطلبات الأمنية للموارد البشرية التي تحدّد وتطبق ضوابط الأمن السيبراني الخاصة بالعاملين واللازمة قبل عملهم، وأثناءه، وعند انتهائه
- إعداد نماذج عقود الموظفين التي تشمل المسؤوليات المتعلّقة بالأمن السيبراني وبنود المحافظة على سرية المعلومات
- إعداد عملية لإجراء المسح الأمني للعاملين على نظم الأمن السيبراني والنظم الحساسة

المسؤوليات

- تتولى الإدارة المعنية بالأمن السيبراني مراقبة تنفيذ متطلبات الأمن السيبراني خلال دورة حياة الموظفين

تعزيز ثقافة الوعي بالأمن السيبراني

التوثيق

- إعداد برامج التوعية بالأمن السيبراني يغطي قنوات عديدة لبناء ثقافة الوعي بالأمن السيبراني ورفع مستوى وعي الأفراد بمخاطر وتهديدات الأمن السيبراني

التقنية

- تطبيق وإعداد نظام لإدارة التعلّم لتقديم محتوى التوعية بالأمن السيبراني، بما يشمل الدورات، ومقاطع الفيديو القصيرة، والنشرات الإعلانية، والمنشورات، والأخبار
- تطبيق وإعداد أداة لعمليات محاكاة التصيد الإلكتروني لإجراء تقييم دوري للتصيد الإلكتروني يُعنى بالموظفين، والمتعاقدين، والأطراف الخارجية

المسؤوليات

- تقوم الإدارة المعنية بالأمن السيبراني تطوير وتقديم محتوى التوعية بالأمن السيبراني وبقياس مستوى الوعي في المنظمة بصورة دورية

حوكمة الهويات وإدارة صلاحيات الدخول

التوثيق

- إعداد سياسة للأمن السيبراني تتضمّن المتطلبات الأمنية لإدارة هويات الدخول والصلاحيات التي تحدّد كيفية إدارة الدخول ومن يمكنه الوصول إلى المعلومات في أيّ ظروف
- وضع سياسة لكلمة المرور تحدّد طريقة إنشاء كلمة المرور، والمتطلبات من حيث تعقيدها، والتخزين والنقل الآمنين، والاختبارات العشوائية الدورية، والإلغاء السريع لحقوق الوصول، والمراقبة المستمرة، وغيرها من المتطلبات
- إعداد إجراءات الدخول الآمن للتحكم في الوصول إلى النظم والتطبيقات، والتحقق من هوية المستخدم
- إعداد المعايير التي تشمل متطلبات التحكم في الوصول الخاصة بالتقنية

التقنية

- تطبيق حلّ لإدارة الدخول يمنح القدرة على إدارة ومراقبة حقوق وصلاحيات الوصول لضمان وصول المستخدمين المصرّح لهم فقط إلى موارد المنظمة بناءً على أدوارهم الوظيفية، أو إداراتهم، أو أيّ من السمات الأخرى التي تبدو مناسبة
- تطبيق حلّ لإدارة الصلاحيات الهامة والحساسة لمراقبة وإدارة الوصول إلى الأصول وموارد الأعمال الحساسة في بيئة المنظمة ككل. وتُعتبر إدارة الصلاحيات الهامة والحساسة راسخة ضمن مبدأ الحدّ الأدنى من الصلاحيات، حيث لا يحظى سوى المستخدمين ذوي الصلاحيات الهامة والحساسة بمسويات الوصول الدنيا اللازمة لأداء مهامهم الوظيفية
- تطبيق حلّ للشبكات الخاصة الافتراضية يسمح للمستخدمين بإنشاء اتصال الشبكة الآمن والمشفّر بالموارد الداخلية عند الاتصال عبر الشبكات العامة أو غير الآمنة، والحرص على تمكين خاصية التحقق من الهوية المتعدد العناصر ضمن الشبكات الخاصة كطبقة دفاع إضافية لمنع إساءة (VPN) الافتراضية الاستخدام وسرقة البيانات الثبوتية (VPN)

المسؤوليات

- تتولى الإدارة المعنية بالأمن السيبراني مراقبة ومراجعة سجلات إدارة هويات الدخول والصلاحيات

معرفة وحماية البيانات

التوثيق

- إعداد سياسة للأمن السيبراني تتضمّن متطلبات حماية البيانات والمعلومات التي تغطي ملكية البيانات والمعلومات، والخصوصية، وآليات التصنيف والترميز، ما يضمن سرية، وسلامة، وتوافر بيانات المنظمة ومعلوماتها
- تحديد الجهات المالكة للبيانات لجميع أنواع البيانات في المنظمة
- تحديد طريقة لتصنيف البيانات لوضع فئات البيانات الحساسة بحيث يمكن تطبيق الضوابط الأمنية بناءً على التصنيفات
- تحديد آلية مرنة (مادية أو رقمية) للترميز في مجال الأمن السيبراني تساهم في تيسير وتبسيط عملية توفير المعلومات اللازمة
- وضع خطة لخصوصية البيانات والمعلومات تستخدم الإجراءات المعتمدة من المنظمة للحفاظ على سلامة البيانات المقيّدة للمنظمة والتحكم في إمكانية الوصول إليها حيث تخضع البيانات لعمليات المعالجة، والتخزين، والنقل
- إعداد سياسة للأمن السيبراني تتضمّن متطلبات الأمن السيبراني التي تغطي إدارة المفاتيح وتشفير البيانات أثناء نقلها وتخزينها حرصًا على استخدام التشفير المناسب الذي يتسم بالكفاءة لحماية الأصول المعلوماتية
- تحديد معيار حلّ التشفير المعتمد الذي يغطي المتطلبات التقنية والتنظيمية

التقنية

- نشر حلّ لاكتشاف البيانات وتصنيفها يقوم بفحص حاويات البيانات لأنواع البيانات التي تُعتبر مهمة، استنادًا إلى معايير الأمن السيبراني أو المتطلبات وبيانات النظام الأوروبي، PCI DSS المتخصصة (مثل معايير أمن البيانات لحماية البيانات، والملكية الفكرية)، وتقسيمها إلى فئات وترميزها بشكل واضح بواسطة التوقيع الرقمي للدلالة على تصنيفها
- إعداد وتطبيق حلّ تشفير الأجهزة الخارجية لتشفير أجهزة وسائط التخزين USB الخارجية بالكامل مثل الأقراص الخارجية الصلبة ومحركات أقراص فلاش ويتمّ تأمين حماية البيانات التي يجري تخزينها ضمن هذه الأجهزة من دون الوصول إلى برمجيات إدارة المفاتيح والتشفير
- تطبيق حلّ تشفير الأجهزة الطرفية لتشفير القرص بالكامل، ويغطي هذا الحلّ تشفير جميع البيانات مثل الملفات، والمجلدات، ونظم التشغيل. ويُعتبر هذا النوع من التشفير مفيدًا في حال عدم توفّر الأمن المادي للنظم

المسؤوليات

- تحدّد الإدارة المعنية بالأمن السيبراني ضوابط الأمن السيبراني اللازمة لكل مستوى من مستويات تصنيف البيانات، وتحرص على توفّر ضوابط حماية البيانات المناسبة لحماية كل من هذه المستويات بناءً على مدى أهمية هذه البيانات

حماية نظم تقنية المعلومات

التوثيق

- إعداد سياسة للأمن السيبراني تتضمّن متطلبات الأمن السيبراني لإدارة الأصول، بما يشمل إدارة الأصول المعلوماتية خلال دورة حياتها بدءًا من إنشائها، مرورًا باستخدامها، وصولًا إلى التخلّص منها
- إعداد سجل للأصول للمنظمة بأكملها يشمل قائمة بجميع الأصول المعلوماتية التي تملكها المنظمة، والاحتفاظ بمثل هذا السجل
- إعداد إجراءات دورة حياة الأصول المعلوماتية التي تشمل كيفية إنشاء هذه الأصول، والاحتفاظ بها، وإتلافها في المنظمة، والمحافظة على مثل هذه الإجراءات. ويضمن ذلك توثيق الإجراءات المرتبطة بالأصول ومعرفة جميع الأطراف المعنيين بهذه الإجراءات
- الإعداد والحفاظ على المعايير والإجراءات التي تشمل متطلبات الأصول الخاصة بالتقنية لمجموعة محدّدة من الأصول المعلوماتية التي تتطلّب اهتمامًا وعناية خاصة، ويتضمّن ذلك إلحاق وإتلاف الأصول وتصنيفها
- الإعداد والاحتفاظ بمعايير التحصين الأمني لوضع الخط الأساس للمتطلبات لضمان حماية النظم وأجهزة معالجة المعلومات (بما في ذلك أجهزة المستخدمين والبنية التحتية)

التقنية

- تطبيق وإعداد أداة لاكتشاف الأصول والاطلاع عليها سعيًا لإلغاء ما يُعرف بتقنية واكتشاف أيّ من الأصول الضارة (shadow IT) المعلومات في الظل
- تطبيق وإعداد قاعدة بيانات لإدارة الإعداد لتوثيق جميع مكوّنات العتاد والبرمجيات الخاصة بالأصول المعلوماتية لدى المنظمة والاحتفاظ بسجل مؤتمت
- نشر حلّ لأمن الأجهزة الطرفية للمساعدة على اكتشاف، وتحليل، وحجب، واحتواء الأنشطة الخبيثة ضمن الأجهزة الطرفية، والحرص على أن تشمل قدرات الحماية من التهديدات المتقدمة المستمرة التي تحمي من البرمجيات الضارة المتقدّمة، والهجمات غير المعروفة مسبقًا، والهجمات المستمرة
- الحصول على حلّ لإدارة التحديثات والإصلاحات التي تقوم بأتمتة، وإدارة، وتثبيت حزم التحديثات والإصلاحات ضمن تطبيقات البرمجيات بصورة دورية. ومن شأن حلّ لإدارة التحديثات والإصلاحات أن يحدّ من إمكانية تعطل النظام أو انتهاكه نتيجة البرمجيات القديمة أو المعيبة

المسؤوليات

- تتولى الإدارة المعنية بالأمن السيبراني مراقبة ومراجعة السجلات الأمنية لأصول المنظمة، بما يشمل السجلات الأمنية لنظم المعلومات وأجهزة معالجة المعلومات

حماية التواصل الإلكتروني

التوثيق

- إعداد سياسة للأمن السيبراني تتضمّن متطلبات الأمن السيبراني لضمان أمن التواصل الإلكتروني التي تفضّل الاستخدام المقبول لنظام البريد الإلكتروني الخاصة بالمنظمة وغيرها من وسائل التواصل الإلكتروني
- وضع المعايير التي تشمل متطلبات أمن البريد الإلكتروني الخاصة بالتقنية للمستخدمين أو فئة المستخدمين المحددين الذين يحتاجون إلى اهتمام ورعاية خاصة

التقنية

- الحصول وتثبيت حلّ لأمن البريد الإلكتروني يستطيع اكتشاف ورصد الرسائل الإلكترونية غير المرغوب فيها أو رسائل التصيد (spam) مثل الرسائل الاقتحامية الإلكتروني. ويجب أن ينطوي الحلّ أيضًا على قدرات الحماية من التهديدات المتقدّمة المستمرة للحماية من التهديدات المتقدّمة والهجمات غير المعروفة مسبقًا، وكذلك إطار سياسة المرسل للحماية من هجمات انتحال الشخصية/ البريد الإلكتروني. وفي حال استلزم الأمر الدخول عن بُعد عن طريقة صفحة موقع البريد الإلكتروني، فيجب تمكين خاصية التحقق من الهوية المتعدد العناصر
- النسخ الاحتياطي وأرشفة البريد الإلكتروني عبر استخدام حلّ يقوم بتخزين وحفظ رسائل البريد الإلكتروني بشكل آمن ويمنح القدرة على استعادة هذه الرسائل عند الحاجة

المسؤوليات

- تتولى الإدارة المعنية بالأمن السيبراني مراقبة ومراجعة سجلات أمن البريد الإلكتروني، وتحرص على توفّر متطلبات حماية البريد الإلكتروني

تطوير وصيانة التطبيقات الآمنة

التوثيق

- تضمين متطلبات الأمن السيبراني في إجراءات إدارة المشاريع وإدارة التغيير، التي يجب أن تشمل المتطلبات التالية: إدارة الثغرات، وتقييمات الإعدادات، واختبار الالتزام بالمعايير الأمنية، وضمان السلامة، والتحصين وحزم التحديثات
- اعتماد المعايير الأمنية لشفرة البرامج والتطبيقات التي يجب اتباعها، بالتزامن مع تطوير التطبيقات داخليًا
- إعداد سياسة للأمن السيبراني تتضمّن معايير أمن التطبيقات مثل متطلبات جدار الحماية لتطبيقات الويب، ومبدأ المعمارية المتعددة المستويات، والبروتوكولات الآمنة، والتحقق من الهوية المتعدد العناصر
- تطوير سياسة للاستخدام الآمن وإرسالها إلى المستخدمين لدى المنظمة
- إعداد معايير أمن التطبيقات الخاصة بالتقنية

التقنية

- تطبيق وإعداد جدار حماية لتطبيقات الويب يقوم بحماية تطبيقات الويب من مجموعة متنوّعة من الهجمات على مستوى طبقات التطبيقات. ويعمل الحلّ القائم على جدار الحماية لتطبيقات الويب على تصفية، ومراقبة، وحجب أيّ من تدفقات البيانات في الشبكات الخبيثة المرتبطة بنظامي بروتوكول نقل النص التشعبي/ بروتوكول نقل النص ومنع أيّ من البيانات، (HTTP/S) التشعبي الآمن غير المصرّح لها بمغادرة التطبيقات
- تعيين إصدارات نظام التحكم في الوصول
- تطبيق برمجيات اختبار التحليل الثابت أو التحليل الديناميكي لأمن التطبيقات لرصد الثغرات الأمنية على مستوى شفرة المصدر للتطبيقات

المسؤوليات

- تتولى الإدارة المعنية بالأمن السيبراني إجراء مراجعة الإعدادات، وتقييم الثغرات، واختبار الالتزام في إطار دورات حياة إدارة المشاريع وإدارة التغيير

حماية الأجهزة المحمولة

التوثيق

- إعداد سياسة للأمن السيبراني تتضمّن متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة والأجهزة الشخصية للعاملين (مبدأ أحضر الجهاز الخاص بك) لتشفير البيانات المخزّنة على الأجهزة الخاصة بالعمل والأجهزة الشخصية، وتحديد إجراءات الحذف الآمن للبيانات والمعلومات بعد انتهاء عمل الموظف
- إعداد سياسة للأمن السيبراني تتضمّن المتطلبات الخاصة بأمن الأجهزة المحمولة التي تغطي انتهاء العلاقة الوظيفية، والأرشفة الآمنة/ الحذف الآمن للبيانات، وتشفير البيانات والمعلومات المخزّنة على الأجهزة المحمولة والأجهزة الشخصية (مبدأ أحضر الجهاز الخاص بك)، استيفاءً لمعايير الحماية من المخاطر السيبرانية، والتعامل مع المعلومات الحساسة بشكل آمن أثناء استخدام الأجهزة الشخصية (مبدأ أحضر الجهاز الخاص بك)

التقنية

- إعداد الحلّ القائم على نظام إدارة الأجهزة المحمولة لإلحاق وتحديث الأجهزة عن بُعد بواسطة إعدادات شبكة الأعمال الداخلية (مثل القيود المتعلّقة والشبكة (VPN) بالشبكات الخاصة الافتراضية اللاسلكية). كما يسمح هذا الحلّ بالإشراف على عدد من الميزات وتقييدها، ونذكر على سبيل المثال تعديل الحساب، وخدمة التجوال، والتحكم في البيانات الخلوية، وإقران الأجهزة، وغيرها من الميزات، في ظل توفير بعض المرونة في ما يخص الأجهزة الشخصية (مبدأ أحضر الجهاز الخاص بك) التي جرى تنظيمها

المسؤوليات

- تتولى الإدارة المعنية بالأمن السيبراني مراقبة تنفيذ متطلبات الأمن السيبراني المتعلّقة باستخدام الأجهزة المحمولة في المنظمة

حماية الشبكات

التوثيق

- إعداد سياسة للأمن السيبراني تتضمّن متطلبات أمن الشبكات التي تحدّد الإرشادات للوصول إلى شبكات الحاسب الآلي
- إعداد المعايير التي تشمل متطلبات أمن الشبكات الخاصة بالتقنية

التقنية

- تثبيت خادم الإنترنت الوسيط (الذي يُعرف أيضًا بخادم الوسيط الأمامي أو خادم الويب الوسيط) ليشكّل صلة وصل بين بوابة العميل ومتصفح الإنترنت وشبكة الإنترنت على سبيل المثال. وينظر هذا الخادم في البيانات الواردة والصادرة عن تطبيق العميل أو الشبكة، ومن ثم يعمل على تطبيق القواعد ذات الصلة
- تطبيق حلّ جدران حماية الجيل التالي التي تُعتبر جدران حماية الفحص العميق لحزم البيانات التي تتخطى فحص المنافذ/ البروتوكولات وحجبها، لإضافة خصائص الفحص والتحكم على مستوى التطبيقات ونظم منع التسلل المتكاملة. ويقدّم نظام مخصص لمنع التسلل خدمة لاكتشاف التهديدات استنادًا إلى التوقيع، وذلك لكشف أنشطة التسلل بصورة استباقية ومحاولة ردعها قبل الوصول إلى هدفها
- لحجب المواقع الإلكترونية (DNS) وتصفية نظام أسماء النطاقات (DNS) استخدام أمن نظام أسماء النطاقات الخبيثة، وتصفية المحتوى المؤذي أو غير المناسب كتدابير مضادة لمواجهة الهجمات السيبرانية حين يستخدم لتوزيع البرمجيات الضارة، والتواصل مع النظم التي تمّ اختراقها، (DNS) المخترقون نظام أسماء النطاقات وتسريب البيانات
- مزامنة الخوادم مع مصدر مركزي لتقنية وبروتوكولات الشبكات يقوم بمزامنة توقيت عميل الحاسب الآلي مع مصدر مركزي وموثوق بهدف منع المهاجمين من التلاعب بالمعلومات حول الوقت

المسؤوليات

- تتولى الإدارة المعنية بالأمن السيبراني مراقبة ومراجعة سجلات أمن الشبكات

الدفاع عن التقنية التشغيلية

التوثيق

- إعداد سياسة للأمن السيبراني تتضمّن المتطلبات الأمنية المادية والمنطقية المرتبطة بأنظمة التحكم الصناعي

التقنية

- تطبيق وإعداد تقنيات الأمن السيبراني اللازمة في ظل مراعاة تلك التي تُعد مؤهلة من قبل صانعي المعدات الأصلية الخاصة بالجهات

المسؤوليات

- تحرص الإدارة المعنية بالأمن السيبراني لأنظمة التحكم الصناعي (في حال ينطبق ذلك على المنظمة) على حماية أنظمة التحكم الصناعي من خلال مراقبة تنفيذ ضوابط الأمن السيبراني لأنظمة التحكم الصناعي

حماية الأجهزة والأصول

التوثيق

- إعداد سياسة للأمن السيبراني تتضمّن متطلبات الأمن المادي لحماية الأجهزة مثل متطلبات الوصول المصرّح به إلى الأماكن الحساسة، ومراقبة الدائرة التلفزيونية المغلقة، وحماية سجلات المراقبة، وإتلاف الأصول الآمن، وأمن أجهزة المنظمة والمتطلبات ذات الصلة

التقنية

- تطبيق وإعداد حلول التحكم في الوصول المادي (المرتبطة باكتشاف، أو منع، أو ردع الوصول غير المصرّح به) من أجل التحكم في قدرة الأشخاص أو الأصول الأخرى على دخول أماكن تحظى بالحماية من خلال سبل التحقق من هوية المستخدم وصلاحيته عند نقاط التحكم في الوصول. ويجب حماية جميع الأجهزة والمرافق التي تملكها المنظمة أو تقوم بتشغيلها
- تمكين المراقبة بالفيديو عبر تثبيت كاميرات الدائرة التلفزيونية المغلقة القائمة على بروتوكولات الإنترنت لتحسين المراقبة الأمنية عبر تسجيل الأحداث، والاحتفاظ بالسجلات، والتكامل مع الحلول الأمنية الأخرى التي تُعنى بالتنبيه وإعداد التقارير
- إزالة مغنطة وسائط التخزين لمحو القرص وإتلاف البيانات المصنفة بشكل آمن

المسؤوليات

- تتولى الإدارة المعنية بالأمن السيبراني تنفيذ متطلبات الأمن السيبراني للأمن المادي

إدارة الثغرات ونقاط الضعف

التوثيق

- إعداد سياسة للأمن السيبراني تشمل متطلبات إدارة الثغرات لفحص واكتشاف الثغرات، وتحديدها، وتصنيفها، وإدارتها، ومعالجتها. وسيتمّ توثيق هذه السياسة، واعتمادها، والإبلاغ عنها، وتنفيذها، ومراجعتها بصورة دورية استنادًا إلى الفترات الزمنية المخطط لها أو عندما تبرز الحاجة إلى إجراء تغييرات
- إعداد معيار لإدارة الثغرات يحدّد العمليات والإجراءات التي تُعنى بفحص واكتشاف الثغرات، ومعالجتها، والإبلاغ عنها
- إعداد منهجية لتصنيف الثغرات من أجل تصنيف عيوب النظم بناءً على مدى أهميتها والمخاطر ذات الصلة وفقًا لمنهجية إدارة المخاطر
- إعداد خطة لفحص واكتشاف الثغرات بصورة دورية لمراجعة، وتحديد، وتصنيف المسائل الأمنية ضمن نظم المنظمة وتطبيق إجراءات المعالجة المناسبة

التقنية

- توريد وإعداد أداة لتقييم الثغرات تقوم بفحص ومراجعة الشبكات، والتطبيقات، والنظم بهدف تقييم مدى تأثرها بنقاط الضعف والثغرات المعروفة، وتقدّم تدابير للتخفيف من أضرارها عند الحاجة

المسؤوليات

- تتولى الإدارة المعنية بالأمن السيبراني فحص واكتشاف الثغرات دوريًا في ما يخص الأصول المعلوماتية للمنظمة

تحديد حالات الانكشاف المحتملة بواسطة اختبار الاختراق

التوثيق

- إعداد سياسة للأمن السيبراني تتضمّن متطلبات اختبار الاختراق لإجراء اختبارات الاختراق وتقييم المتطلبات الأمنية لنظم المنظمة لرصد وتحديد حالات الانكشاف المحتملة
- إعداد معيار لاختبارات الاختراق لتحديد الإجراءات المعنية بإجراء الاختبارات، وتحديد النهج وسيناريوهات الهجمات
- إعداد خطة لإجراء اختبارات الاختراق دوريًا لضمان تقييم المتطلبات الأمنية لنظم المنظمة واكتشاف الثغرات القابلة للاستغلال

التقنية

- الاستفادة من مجموعة من أدوات اختبار الاختراق لمساعدة الفاحص في مناقشة سيناريوهات الهجمات والكشف عن الثغرات على مستوى الشبكات، والتطبيقات، والأجهزة الطرفية

المسؤوليات

- تتولى الإدارة المعنية بالأمن السيبراني إجراء اختبارات الاختراق دوريًا في ما يخص الأصول المعلوماتية للمنظمة

مراقبة واكتشاف تهديدات الأمن السيبراني

التوثيق

- إعداد سياسة للأمن السيبراني تتضمّن متطلبات إدارة سجلات الأحداث ومراقبة الأمن السيبراني للحدّ من الانتهاكات الأمنية المحتملة من خلال ضمان المراقبة المستمرة، واكتشاف الأحداث الأمنية وتحليلها في الوقت المناسب
- إعداد معيار لإدارة سجلات الأحداث ومراقبة الأمن السيبراني لتحديد تسجيل الأحداث، وصيغة السجلات، ومصادر الأحداث، ومراقبة الأحداث، والتنبيهات، ومراجعة سجلات الأحداث، والاحتفاظ بالسجلات، إلخ

التقنية

- دمج حلّ لنظام لإدارة سجلات الأحداث ومراقبة الأمن السيبراني يقدّم نظرة شاملة وخدمة المراقبة في الوقت الفعلي للوضع الأمني للمنظمة عبر جمع سجلات الأحداث من مختلف نظم المعلومات كي تتمكّن الفرق الأمنية من اكتشاف الأحداث الأمنية وإدارتها

المسؤوليات

- تتولى الإدارة المعنية بالأمن السيبراني الإشراف على تفعيل سجلات الأحداث الخاصة بالحسابات ذات الصلاحيات الهامة والحساسة على الأصول والمعلوماتية وأحداث عمليات الدخول عن بُعد. ويهدف ذلك إلى مراقبة وتحليل الأحداث للاكتشاف المبكر للهجمات السيبرانية

تعزيز عمليات الأمن السيبراني والمعلومات الاستباقية

التوثيق

- إعداد سياسة للأمن السيبراني تتضمّن متطلبات إدارة تهديدات الأمن السيبراني لضمانة قدرة المنظمة على إدارة التهديدات وامتلاك وسائل الحماية المناسبة من خلال تحديد وتحليل التهديدات السيبرانية المحتملة وغير المكتشفة من حيث الجهات التي تقف وراء هذه التهديدات، ودوافعها وقدراتها، ومتجهات التهديدات، والهجمات
- إعداد معيار لإدارة تهديدات الأمن السيبراني لتحديد الوسائل المناسبة للاحتفاظ بالمعلومات الاستباقية

التقنية

- الاشتراك في مصدر ذائع الصيت للمعلومات الاستباقية للسماح لصانعي القرارات الأمنية بالتركيز على التهديدات الهامة في الوقت الحاضر، والحدّ من التهديدات التي تشنّها الجهات ذات التغييرات السريعة، واكتشاف الهجمات الناشئة، والحدّ من سطح مخاطر التهديدات القائمة على مستوى المنظمة. ربط الحلول الأمنية بمصادر المعلومات الاستباقية الخارجية للحصول على الاستخبارات القابلة للتطبيق، والمعلومات والتحليلات المتقدّمة، ومؤشرات الانتهاكات الأمنية، ومؤشرات الهجمات، وتقارير الهجمات المحتملة

المسؤوليات

- تتولى الإدارة المعنية بالأمن السيبراني جمع وتحليل المعلومات الاستباقية التي تمّ جمعها وتحديد التهديدات السيبرانية وتكتيكات الجهات، والتقنيات والإجراءات

الاستجابة لحوادث الأمن السيبراني

التوثيق

- تطوير سياسة للأمن السيبراني تتضمّن متطلبات إدارة الحوادث لضمان الاستجابة إلى حوادث الأمن السيبراني والإبلاغ عنها في الوقت المناسب وبشكل ملائم
- إعداد كتب قواعد للاستجابة للحوادث لتوفير التوجيهات بشأن تطوير خطط الاستجابة للحوادث، والتعافي من الكوارث، واستمرارية الأعمال، وتحديد تصنيف الحوادث وترتيبها بحسب الأولويات، والتبليغ عن الحوادث
- إعداد خطة للاستجابة إلى الحوادث لتحديد حوادث الأمن السيبراني، والحدّ منها، والتعافي منها بشكل مناسب

التقنية

- تطبيق منصة لإدارة الحوادث لأتمتة، وتوجيه، وتقييم عملية الاستجابة للحوادث. ويساعد النظام المحللين الأمنيين من خلال تزويدهم بالأدوات التي تُعنى بإدارة حالات الحوادث، والنظام المتكامل لإدارة سجلات الأحداث ومراقبة الأمن السيبراني وغيرها من الأدوات وخدمات الاستجابة المؤتمتة عبر استخدام كتب القواعد الأمنية

المسؤوليات

- تتولى الإدارة المعنية بالأمن السيبراني اكتشاف الحوادث السيبرانية، وتحليلها، والاستجابة لها، وتحرص على تبليغ الهيئة الوطنية للأمن السيبراني بالحوادث السيبرانية

تطوير خطط التعافي وضمان استمرارية الخدمات

التوثيق

- إعداد سياسة للأمن السيبراني تضمّنت جوانب استمرارية الأعمال المتعلّقة بالأمن السيبراني للتأكد من استمرارية النظم والإجراءات بعد وقوع الحوادث الأمنية
- إعداد سياسة للأمن السيبراني تتضمّن متطلبات إدارة النسخ الاحتياطية للاحتفاظ بالسجلات والبرمجيات، وتحديد وتيرة عمليات النسخ الاحتياطي بناءً على تقلبات البيانات، وامتلاك نسخة واحدة يمكن استعادتها بالكامل وتكون مخزّنة خارج الموقع
- إجراء فحص دوري لخطة النسخ الاحتياطي أو بعد حدوث تغيير كبير على مستوى الإجراءات أو العمليات
- إعداد استراتيجية لتجاوز الفشل تدعم النظام الأساسي في حال وقوع أعطال والسماح باستئناف توافر النظم حين تعجز آليات تجاوز الفشل عن إبقاء النظم متوافرة
- إعداد خطة للتعافي من الكوارث وخطط الاستجابة للحوادث لتفصيل كيفية الاستجابة للحوادث غير المخطط لها مثل الهجمات السيبرانية، والكوارث الطبيعية، وانقطاع التيار الكهربائي، وغيرها من الحوادث. وتحدّد خطة التعافي من الكوارث الاستراتيجيات حول كيفية التخفيف من آثار الكوارث، والسماح للمنظمة باستئناف العمليات الرئيسية بسرعة أو مواصلة العمليات كما لو أنه لم تقع أيّ كارثة

التقنية

- استخدام أجهزة معالجة المعلومات المتكررة للتأكد من استمرارية الأعمال بالكامل، في حال وقوع كارثة، حيث أن توقف الأعمال قد يؤدي إلى تكبد المنظمة خسائر فادحة
- تطبيق نظام لإدارة النسخ الاحتياطية للاحتفاظ بنسخة وأرشفة البيانات الهامة وحمايتها من فقدان البيانات العرضي، وتلفها، والوصول غير المصرّح به

المسؤوليات

- تحرص الإدارة المعنية بالأمن السيبراني على تضمين متطلبات الأمن السيبراني والهجمات السيبرانية في خطط/ استراتيجيات استمرارية الأعمال والتعافي من الكوارث

إدارة وحماية الأمن السيبراني المتعلّق بالحوسبة السحابية والاستضافة

التوثيق

- إعداد سياسة للأمن السيبراني تتضمّن متطلبات الأمن السيبراني للحوسبة السحابية والاستضافة

التقنية

- تطبيق وإعداد التقنيات اللازمة للأمن السيبراني

المسؤوليات

- تحرص الإدارة المعنية بالأمن السيبراني على أن تحظى البيئة السحابية للمنظمة بالحماية من خلال مراقبة تنفيذ متطلبات الأمن السيبراني للحوسبة السحابية

تضمين متطلبات السيبراني في الاتفاقيات مع الأطراف الخارجية

التوثيق

- إعداد سياسة للأمن السيبراني تتضمّن متطلبات الأمن السيبراني للأطراف الخارجية للتعاقد مع الأطراف الخارجية والخدمات المدارة
- دمج متطلبات الأمن السيبراني في اتفاقيات مستوى الخدمة مثل بنود المحافظة على سرية المعلومات، والحذف الآمن من قِبل الطرف الخارجي لبيانات المنظمة عند انتهاء الخدمة، وإجراءات التواصل في حال حدوث حادثة أمن سيبراني، ومتطلبات الالتزام بالأمن السيبراني

المسؤوليات

- تحرص الإدارة المعنية بالأمن السيبراني على أن تكون متطلبات الأمن السيبراني مدمجة ضمن اتفاقيات مستوى الخدمة

تواصل معنا

هيثم الجوهري

شريك، قسم الأمن السيبراني

haitham.al-jowhari@pwc.com

+966 54621 8888

علي مسلماني

مدير رئيسي، قسم الأمن السيبراني

ali.mouslmani@pwc.com

+971 54793 4058

محمد عايش

رئيس، قسم الأمن السيبراني

mohammed.ayesh@pwc.com

+966 54767 7828

عبدالرحمن كردي

مدير، قسم الأمن السيبراني

abdulrahman.kurdi@pwc.com

+966 54766 8395

نبذة عن بي دبليو سي

هدفنا في بي دبليو سي هو تعزيز الثقة في المجتمع وحل المشاكل الهامة. بي دبليو سي هي شبكة شركات متواجدة في ١٥٦ بلداً ويعمل لديها ٢٩٥,٠٠٠ موظف ملتزمون بتوفير أعلى معايير الجودة في خدمات التدقيق والاستشارات والضرائب.

www.pwc.com لمزيد من المعلومات، يرجى زيارة موقعنا الالكتروني

تأسست بي دبليو سي في الشرق الأوسط منذ ٤٠ عاماً ولديها ٢٢ مكتباً في ١٢ دولة، حيث يعمل بها حوالي (٧٠٠٠) .موظف. (www.pwc.com/me).

بي دبليو سي تشير إلى شبكة بي دبليو سي و/ أو واحدة أو أكثر من الشركات الأعضاء فيها، كل واحدة منها هي كيان .www.pwc.com/structure قانوني مستقل. للمزيد من المعلومات يرجى زيارة موقعنا الالكتروني