هذا المربع مخصّص لأغراض توجيهية. احذف جميع المربعات التوجيهية بعد تعبئة النموذج. يجب تحرير البنود الملوّنة باللون الأزرق بصورة مناسبة. ويجب إزالة التظليل الملون بعد إجراء التعديلات.

أدخل شعار الجهة بالضغط على الصورة الموضحة.

نموذج أدوار ومسؤوليات الأمن السيبراني

استبدل <اسم الجهة> باسم الجهة في مجمل صفحات الوثيقة. وللقيام بذلك، اتبع الخطوات التالية:

1. اضغط على مفتاحي "Ctrl" و"H" في الوقت نفسه.
2. أضف "<اسم الجهة>" في مربع البحث عن النص.
3. أدخل الاسم الكامل لجهتك في مربع "استبدال" النص.
4. اضغط على "المزيد" وتأكّد من اختيار "Match case".
5. اضغط على "استبدل الكل".
6. أغلق مربع الحوار.

اختر التصنيف

التاريخ: اضغط هنا لإضافة نص

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

اعتماد الوثيقة

الدور	الاسم	التاريخ	التوقيع
اختر الدور	<أدخل الاسم الكامل للشخص>	اضغط هنا لإضافة نص	<أدخل التوقيع>

نسخ الوثيقة

النسخة	التاريخ	عُدّل بواسطة	أسباب التعديل
<أدخل رقم النسخة>	اضغط هنا لإضافة نص	<أدخل الاسم الكامل للشخص>	<أدخل وصف التعديل>

قائمة المحتويات

مقدمة

تم تطوير هذه الوثيقة لتحديد المسؤوليات الخاصة بتطبيق برامج ومتطلبات الأمن السيبراني ودعمه وتعزيزه في <اسم الجهة>، ويجب على جميع الأطراف المشاركة في تطبيق برامج ومتطلبات الأمن السيبراني فهم أدوارهم والقيام بمسؤولياتهم المتعلقة بالأمن السيبراني في <اسم الجهة>.

الأهداف

تهدف هذه الوثيقة إلى التأكد من أن جميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني في <اسم الجهة> على دراية بمسؤولياتهم في تطبيق برامج ومتطلبات الأمن السيبراني في <اسم الجهة> والجهات التابعة لها.

وتهدف هذه الوثيقة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-٤-١ والضابط رقم ١-٩-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

الأدوار والمسؤوليات المتعلقة بالأمن السيبراني

<صاحب الصلاحية>

#	المسؤوليات
1	تأسيس <الإدارة المعنية بالأمن السيبراني> وضمان استقلاليتها لعدم تضارب المصالح، وتعيين <رئيس الإدارة المعنية بالأمن السيبراني> ويجب أن يكون سعودي الجنسية.
2	تأسيس اللجنة الإشرافية للأمن السيبراني.
3	الموافقة على وثيقة اللجنة الإشرافية للأمن السيبراني.
4	تخصيص الميزانية الكافية لمتطلبات الأمن السيبراني بما في ذلك ميزانية الموارد البشرية.
5	اعتماد استراتيجية الأمن السيبراني بعد رفعها للّجنة الإشرافية للأمن السيبراني.
6	اعتماد سياسات الأمن السيبراني بعد رفعها للّجنة الإشرافية للأمن السيبراني.
7	اعتماد حوكمة الأمن السيبراني ومنهجية إدارة المخاطر السيبرانية بعد رفعهما للّجنة الإشرافية للأمن السيبراني.
8	اعتماد منهجية إدارة المخاطر السيبرانية بعد رفعها للّجنة الإشرافية للأمن السيبراني.
9	الاطلاع على تقارير حالة الأمن السيبراني دورياً، وتوفيرالدعم المطلوب.

اختر التصنيف

أعضاء اللجنة الإشرافية للأمن السيبراني

#	المسؤوليات
1	متابعة المبادئ (Principles) والمتطلبات التشغيلية وفقاً للوثيقة المنظمة للّجنة الإشرافية للأمن السيبراني.
2	ترسيخ مبادئ المساءلة والمسؤولية والصلاحية من خلال تحديد الأدوار والمسؤوليات بهدف حماية الأصول المعلوماتية والتقنية الخاصة بـ<اسم الجهة>.
3	التأكد من وجود منهجية معتمدة لإدارة وتقييم المخاطر السيبرانية ومستوى المخاطر المقبول (Risk Appetite) لدى <اسم الجهة>، ومراجعتها بشكل مستمر أو عند حدوث أي تغيير جوهري في مستوى المخاطر المقبول.
4	الموافقة على إجراءات مخاطر الأمن السيبراني ودعمها ومراقبتها.
5	الموافقة على حوكمة الأمن السيبراني ودعمها ومراقبتها.
6	مراجعة استراتيجية الأمن السيبراني لضمان توافقها مع الأهداف الاستراتيجية لـ<اسم الجهة> قبل اعتمادها.
7	اعتماد تنفيذ استراتيجية الأمن السيبراني ودعمه ومراقبته.
8	الموافقة على تطبيق سياسات الأمن السيبراني ودعمه ومراقبته.
9	اعتماد مبادرات ومشاريع الأمن السيبراني (مثل: برنامج التوعية بالأمن السيبراني، وحماية البيانات والمعلومات، وغيرها) ودعمها ومراقبتها.
10	الموافقة على مؤشرات الأداء (Key Performance Indicators "KPIs") ومتابعتها، والتأكد من فعاليتها لأعمال <الإدارة المعنية بالأمن السيبراني> والعمل على رفع مستوى الأداء.
11	متابعة تقارير إدارة حزم البيانات والإعدادات ومراقبتها دورياً.
12	متابعة إدارة حوادث الأمن السيبراني ودعمها.
13	مراجعة التقارير الدورية الصادرة من <الإدارة المعنية بالأمن السيبراني> والتي تشتمل على مشاريع الأمن السيبراني، والحالة العامة لوضع الأمن السيبراني، والمخاطر السيبرانية الداخلية التي قد تؤثر على عمل <اسم الجهة>، وكذلك المخاطر السيبرانية الخارجية والتي قد تؤثر بشكل مباشر أو غير مباشر على أعمال <اسم الجهة>، وتقديم الدعم اللازم لمواجهة تلك المخاطر.

#	المسؤوليات
14	مراجعة التقارير الخاصة بمخاطر الأمن السيبراني ومتابعة معالجتها وتقديم الدعم اللازم لمعالجتها أو العمل على تقليلها.
15	مراجعة التقارير الأمنية الخاصة بحوادث الأمن السيبراني وتقديم التوصيات بشأنها.
16	مراجعة طلبات الاستثناءات الخاصة بالأمن السيبراني وتقديم التوصيات بشأنها.
17	متابعة تقارير حالة حزم التحديثات والإصلاحات الأمنية، وتقييم الثغرات الأمنية على جميع الأصول التقنية والمعلوماتية والتأكد من معالجتها.
18	مراجعة نتائج تدقيق الأمن السيبراني الداخلي والخارجي، والتأكد من وجود خطة مناسبة لمعالجة الملاحظات المكتشفة ومتابعتها وتقديم الدعم اللازم لمعالجتها.
19	رفع التقارير الدورية عن حالة الأمن السيبراني والدعم المطلوب لصاحب الصلاحية.
20	مراجعة حالة الالتزام بالمتطلبات الداخلية للجهة والمتطلبات التشريعية الصادرة من الهيئة الوطنية للأمن السيبراني.

<رئيس الإدارة المعنية بالأمن السيبراني>

#	المسؤوليات
1	الإشراف على تطوير استراتيجية الأمن السيبراني وتحديثها.
2	الإشراف على تطوير وتنفيذ منهجيات وإجراءات مراقبة حوادث الأمن السيبراني، وتوجيه أنشطة الأمن السيبراني ومتابعتها بشكل مستمر ورفع التقارير الخاصة بها.
3	الإشراف على تطوير وتحديث منهجية وإجراءات إدارة مخاطر الأمن السيبراني.
4	التأكد من تطوير معايير وإجراءات الأمن السيبراني والموافقة عليها وتطبيقها.
5	الإشراف على تطوير سياسات الأمن السيبراني وتحديثها بناءً على متطلبات الأمن السيبراني.
6	التأكّد من توافق إدارة مخاطر الأمن السيبراني مع إدارة المخاطر في <اسم الجهة>.
7	تقديم حلول وتوصيات حول الأمن السيبراني لتقليل المخاطر السيبرانية على الأصول المعلوماتية والتقنية.

#	المسؤوليات
8	تقديم التوجيهات والدعم اللازم ومعالجة المسائل المتعلقة بتخطيط وإدارة الموارد البشرية الخاصة بالأمن السيبراني (مثل: التوظيف والاحتفاظ بالموظفين والتدريب).
9	الإشراف على تحديد متطلبات الأمن السيبراني وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة والتأكد من الالتزام بها.
10	الإشراف على حوادث الاستجابة للأمن السيبراني ورفع التقارير الخاصة بها.
11	الإشراف على التقييم المستمر للثغرات ومتابعة تطبيق حزم التحديثات الأمنية والإعدادات.
12	الإشراف على جمع وتحليل المعلومات الاستباقية المتعلقة بالأمن السيبراني من المصادر الوطنية أو المصادر الدولية.
13	الإشراف على إجراء اختبارات اختراق دورية على جميع الخدمات المقدمة خارجياً ومكوناتها التقنية لتقييم مستوى الأمن السيبراني.
14	الإشراف على إعداد مبادئ تصميم الأمن السيبراني، وتصاميم الأمن السيبراني للأنظمة والشبكات، ومعمارية الأمن السيبراني، مع ضمان المواءمة مع المعمارية المؤسسية (Enterprise Architecture).
15	الإشراف على إدارة الوصول المنطقي (Logical Access) إلى الأصول المعلوماتية والتقنية لـ<اسم الجهة> من خلال تحديد متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات في <اسم الجهة> وتوثيقها وتطبيقها.
16	الإشراف على إعداد الميزانية الخاصة بتنفيذ مبادرات ومشاريع الأمن السيبراني.
17	التأكد من مراجعة متطلبات الأمن السيبراني دورياً.
18	توفير الدعم والإشراف على إعداد آلية مناسبة لقياس مؤشرات الأداء (KPIs) لأعمال الأمن السيبراني ومشاركتها مع اللجنة الإشرافية للأمن السيبراني.
19	التواصل مع الهيئة الوطنية للأمن السيبراني وإدارة العلاقة معها.
20	الإشراف على برامج الأمن السيبراني ومنها برنامج التوعية بالأمن السيبراني.

موظفو <الإدارة المعنية بالأمن السيبراني>

#	المسؤوليات
1	تطوير سياسات وإجراءات ومعايير الأمن السيبراني ومراجعتها سنوياً.
2	تحديد منهجية وإجراءات إدارة مخاطر الأمن السيبراني وتطبيقها ومراجعتها دورياً.
3	التأكد من تطبيق سياسات وإجراءات ومعايير الأمن السيبراني.
4	تطبيق عملية إدارة مخاطر الأمن السيبراني وتنفيذها.
5	إجراء تقييمات المخاطر، ومتابعة وضع المخاطر والإجراءات التي تم اتخاذها بالتنسيق مع أصحاب المصلحة.
6	تحديد المسؤوليات المتعلقة بالمخاطر بالتنسيق مع أصحاب المصلحة.
7	إعداد تقارير تقييم المخاطر واعتمادها من قبل <رئيس الإدارة المعنية بالأمن السيبراني>.
8	تنفيذ برنامج الالتزام بالأمن السيبراني ومراجعته سنوياً.
9	تطوير برنامج التوعية والتدريب بالأمن السيبراني.
10	تطبيق برنامج التوعية والتدريب بالأمن السيبراني بالتنسيق مع <الإدارة المعنية بالموارد البشرية> وقياس مدى التزام العاملين بالتوعية بالأمن السيبراني.
11	إعداد تقارير الالتزام بمتطلبات الأمن السيبراني واعتمادها من قبل <رئيس الإدارة المعنية بالأمن السيبراني>.
12	القيام بأنشطة المراقبة وإعداد التقارير المتعلقة بالالتزام بالأمن السيبراني.
13	توفير نظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني (SIEM) ومراقبته.
14	متابعة أنظمة مراقبة الأمن السيبراني للتأكد من استقرارها وتوافرها، وتقديم تقارير لوصف حالتها.
15	جمع أحداث الأمن السيبراني في الأصول المعلوماتية والتقنية في نظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني (SIEM)، وتحليل السجلات، وتحديد مخاطر الأمن السيبراني.
16	التعامل مع حوادث الأمن السيبراني ومتابعة إغلاقها، وتصعيد الأحداث القائمة التي تتجاوز اتفاقية مستوى الخدمة المحددة.
17	التقييم المستمر للثغرات ومتابعة تطبيق حزم التحديثات الأمنية والإعدادات.

#	المسؤوليات
18	إجراء اختبارات اختراق دورية على جميع الخدمات المقدمة خارجياً ومكوناتها التقنية لتقييم مستوى الأمن السيبراني.
19	إعداد مبادئ تصميم الأمن السيبراني وتصاميم الأمن السيبراني للأنظمة والشبكات ومعمارية الأمن السيبراني، مع ضمان المواءمة مع المعمارية المؤسسية (Enterprise Architecture).
20	إدارة الوصول المنطقي (Logical Access) إلى الأصول المعلوماتية والتقنية لـ<اسم الجهة> من خلال تحديد متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات في <اسم الجهة> وتوثيقها وتطبيقها.

<رئيس الإدارة المعنية بتقنية المعلومات>

#	المسؤوليات
1	التأكد من التزام <الإدارة المعنية بتقنية المعلومات> بجميع متطلبات الأمن السيبراني.
2	قيادة وتوجيه موظفي <الإدارة المعنية بتقنية المعلومات> من خلال الإشراف على التدريب والتوعية والتثقيف بالأمن السيبراني تماشياً مع مسؤولياتهم.
3	المشاركة والمساهمة في تطوير إطار وإجراءات وعمليات إدارة المخاطر وتطبيقها.
4	اعتماد وسائل يدوية (غير آلية) للتحديثات والإصلاحات في حال لم تكن الأدوات الآلية المستخدمة في <اسم الجهة> مدعومة.
5	الإشراف والمتابعة الدورية لتنفيذ الحلول الآلية لإدارة حزم التحديثات والإصلاحات.
6	مراجعة فاعلية وكفاءة إدارة التحديثات والإصلاحات في الأنظمة الحساسة المتعلقة بتقنية المعلومات.
7	التأكد من إشراك <الإدارة المعنية بالأمن السيبراني> في جميع المسائل المتعلقة بالأصول المعلوماتية والتقنية، وإدارة المشاريع، والمشتريات.
8	التأكد من إشراك <الإدارة المعنية بالأمن السيبراني> لضمان حماية الأصول المعلوماتية والتقنية لـ<اسم الجهة> على النحو المطلوب.
9	التأكّد من مراجعة عقود الصيانة الحالية مع موردي أنظمة تقنية المعلومات و/أو الأنظمة الحسّاسة لتزويد <اسم الجهة> بأحدث الإصدارات من حزم التحديثات والإصلاحات.
10	الإشراف على سرعة تطبيق التوصيات للتقليل من مخاطر الأمن السيبراني.

اختر التصنيف

#	المسؤوليات
11	الإشراف على إدارة عمليات التشغيل للأصول التقنية المتعلقة بالأمن السيبراني.

موظفو <الإدارة المعنية بتقنية المعلومات>

#	المسؤوليات
1	تطبيق متطلبات الأمن السيبراني المتعلقة بـ<الإدارة المعنية بتقنية المعلومات>، بما في ذلك سياسات الأمن السيبراني وإجراءاته وعملياته ومعاييره وإرشاداته.
2	معالجة الثغرات ومتابعة تطبيق حزم التحديثات الأمنية والإعدادات.
3	تطبيق متطلبات الأمن السيبراني فيما يتعلق بطبيعة عمل الموظف المعني.
4	تصعيد أي أنشطة مشبوهة أو مخاوف تتعلق بالأمن السيبراني إلى <الإدارة المعنية بالأمن السيبراني> والإبلاغ عنها.
5	المساعدة في تقديم مدخلات لأنشطة عمليات إطار إدارة المخاطر والوثائق ذات العلاقة.
6	التنسيق مع <الإدارة المعنية بالأمن السيبراني> حول جميع المسائل المتعلقة بالأصول المعلوماتية والتقنية وإدارة المشاريع.
7	التنسيق مع <الإدارة المعنية بالأمن السيبراني> لضمان حماية الأصول المعلوماتية والتقنية لـ<اسم الجهة> وتأمينها على النحو المطلوب.
8	مراجعة عقود الصيانة الحالية مع موردي أنظمة تقنية المعلومات والأنظمة الحسّاسة للتأكد من تزويد <اسم الجهة> بأحدث الإصدارات من حزم التحديثات والإصلاحات.

<مسؤول تطوير التطبيقات>

#	المسؤوليات
1	الإشراف على تنفيذ متطلبات الأمن السيبراني المتعلقة بتطوير التطبيقات في <اسم الجهة>.
2	التنسيق مع فريق الأمن السيبراني حول المسائل المتعلقة بالأمن السيبراني التي تؤثر على <الإدارة المعنية بتطوير التطبيقات>.

#	المسؤوليات
3	التأكد من تطبيق معايير الأمن السيبراني المعتمدة لتطوير التطبيقات، مثل (Open Web Application Security Project "OWASP").
4	الإشراف على تطبيق معايير وأدوات الاختبار الأمني (Testing Standards) والمعايير الأمنية لشفرة البرامج والتطبيقات (Coding Standards)، بما في ذلك الفحص العشوائي (Fuzzing) لأدوات التحليل الثابت للشفرات (Static Code Analysis) وإجراء مراجعات لشفرة البرامج والتطبيقات (Code Reviews).
5	تحديد حزم التحديثات والإصلاحات وتوثيقها والتأكد من سلامتها قبل تنصيبها.
6	التأكد من توثيق الشفرة المصدرية لعمليات التطوير الداخلية والخارجية (أي من خلال طرف خارجي) للتطبيقات في <اسم الجهة> لتمكين عمليات التتبع والمراجعة في إدارة الثغرات.
7	التأكد من البرمجة الآمنة من خلال التأكد من معالجة الأخطاء وتحديد الأخطاء المحتملة في التشفير للحد من الثغرات.
8	التأكد من معالجة جميع الثغرات في مرحلة بيئة الاختبار (Software Acceptance Phase)، بما في ذلك معايير الإتمام (Completion Criteria)، وقبول المخاطر وتوثيقها، والمعايير المشتركة (Common Criteria)، وأساليب الاختبار المستقل (Independent Testing)، وإطلاع <الإدارة المعنية بالأمن السيبراني> على جميع مشاريع تطوير التطبيقات.
9	التأكد من تحديد الخدمات والوظائف المتعلقة بالأمن السيبراني (مثل: التشفير، والتحكم بالوصول، وإدارة الهوية) واستخدامها للحد من فرص الاستغلال.

المعنيون بتطوير التطبيقات

#	المسؤوليات
	بالإضافة إلى جميع المسؤوليات المذكورة لموظفي <الإدارة المعنية بتقنية المعلومات>، يتولّى المعنيون بتطوير التطبيقات المسؤوليات التالية:
1	تنفيذ متطلبات الأمن السيبراني المتعلقة بتطوير التطبيقات في <اسم الجهة>، واتباع المعايير والإجراءات المعتمدة في تطوير التطبيقات (مثل: معايير التطوير الآمن للتطبيقات).
2	متابعة عمليات إدارة المشاريع والتغييرات في <اسم الجهة>، وذلك بالنسبة لجميع التغييرات التي تنطبق على التطبيقات الخاصة بـ<اسم الجهة>.

#	المسؤوليات
3	تحديد التحديثات والإصلاحات اللازمة للبرامج وتوثيقها.
4	إجراء البرمجة الآمنة، ومعالجة الأخطاء، وتحديد الأخطاء المحتملة في التشفير للحد من الثغرات.
5	تطبيق معايير وأدوات الاختبار الأمني والمعايير الأمنية لشفرة البرامج والتطبيقات، بما في ذلك الفحص العشوائي لأدوات التحليل الثابت للشفرات، وإجراء مراجعات لشفرة البرامج والتطبيقات.
6	تحديد وتوثيق التحديثات والإصلاحات اللازمة للبرامج، والإصدارات التي تكون خلالها البرامج عرضة للثغرات.

<مسؤول عمليات تقنية المعلومات>

#	المسؤوليات
1	تنسيق فترات الصيانة حسب الأولوية وتخطيطها وتحديد موعدها من أجل تثبيت التحديثات والإصلاحات وفقاً لسياسة إدارة المشاريع والتغييرات المعتمدة في <اسم الجهة> بما لا يؤثر على الأمن السيبراني للأصول.
2	الإشراف على الحلول الآلية لإدارة حزم التحديثات والإصلاحات، والتأكد من إجراء التحديثات اليدوية في حال كانت التحديثات والإصلاحات الآلية غير مدعومة.
3	الإشراف على النسخ الاحتياطية المنتظمة واختبارات النسخ الاحتياطية.
4	الإشراف على تنفيذ متطلبات الأمن السيبراني المتعلقة بعمليات تقنية المعلومات في <اسم الجهة>.
5	التأكد من اختبار تحديثات وإصلاحات الأصول المعلوماتية والتقنية قبل النشر.
6	التأكد من نجاح تثبيت التحديثات والإصلاحات على الأنظمة.
7	التأكد من تنفيذ سياسات الأمن السيبراني المتعلقة بالأصول المعلوماتية والتقنية الخاصة بـ<اسم الجهة> (مثل نموذج سياسة أمن أجهزة المستخدمين، ونموذج سياسة أمن الخوادم، وغيره).
8	تحديد وترتيب الأولويات والقدرات لاستعادة الأنظمة ووحدات الأعمال الأساسية اللازمة كلياً أو جزئياً بعد وقوع حدث كارثي يؤثر على الأنظمة واستمرارية الأعمال.
9	تحديد المستويات الملائمة لتوافر المعلومات في الأنظمة، وذلك استناداً إلى الوظائف الأساسية للنظام المعني، مع ضمان أن متطلبات النظام تحدد متطلبات التعافي من الكوارث واستمرارية الأعمال، بما

#	المسؤوليات
	في ذلك أي متطلبات موقع بديل (Fail-over Site)، ومتطلبات النسخ الاحتياطية، ومتطلبات القدرة على الدعم لاستعادة واسترداد النظام.
10	الإشراف على اختبار كفاءة خطة التعافي من الكوارث والمشاركة في اختبار كفاءة خطة استمرارية الأعمال.

المعنيون بعمليات تقنية المعلومات

#	المسؤوليات
بالإضافة إلى جميع المسؤوليات المذكورة لموظفي <الإدارة المعنية بتقنية المعلومات>، يتولّى المعنيون بعمليات تقنية المعلومات المسؤوليات التالية:	
1	المساعدة في التنسيق مع <الإدارة المعنية بالأمن السيبراني> حول المسائل المتعلقة بالأمن السيبراني التي تؤثر على الإدارة المعنية بعمليات تقنية المعلومات.
2	تنفيذ متطلبات الأمن السيبراني المتعلقة بعمليات تقنية المعلومات في <اسم الجهة>.
3	تنفيذ الحلول الآلية لإدارة حزم التحديثات والإصلاحات.
4	توفير النسخ الاحتياطية واختبارها دورياً.
5	تنفيذ الحلول الآلية لإدارة حزم التحديثات والإصلاحات، والتأكد من إجراء التحديثات اليدوية متى ما كانت التحديثات والإصلاحات الآلية غير مدعومة.
6	تفعيل وحماية السجلات المناسبة ودمجها مع نظام إدارة السجلات المركزي.
7	تهيئة جميع برامج الإدارة وبرامج الحماية ونظام التشغيل على الأصول المعلوماتية والتقنية.
8	الإشراف على صلاحيات الوصول وحسابات المستخدمين للأصول المعلوماتية والتقنية حسب السياسة الخاصة بها.
9	مراعاة عزل الأصول المعلوماتية والتقنية والتقسيم المنطقي لأجزاء الشبكات بشكل آمن.
10	المشاركة في إدارة التهديدات والحوادث في أنظمة تقنية المعلومات في المراحل المعنية بها (مثل: مراحل الاحتواء (Containment)، والاستئصال (Eradication)، والتعافي أو الاستعادة ((Recovery).

#	المسؤوليات
11	المساعدة في تحديد وترتيب أولويات قدرات الأنظمة ووحدات الأعمال الأساسية اللازمة لاستعادة النظام المعني كلياً أو جزئياً بعد وقوع حدث كارثي يتسبب في فشل متعلق بالأمن السيبراني.
12	المساعدة في تحديد المستويات الملائمة لتوافر المعلومات في الأنظمة، وذلك استناداً إلى الوظائف الأساسية للنظام المعني، مع ضمان أن متطلبات النظام تحدد متطلبات التعافي من الكوارث واستمرارية الأعمال، بما في ذلك أي متطلبات موقع بديل (Fail-over Site)، ومتطلبات النسخ الاحتياطية، ومتطلبات القدرة على الدعم لاستعادة النظام واسترداده.

<رئيس الإدارة المعنية بالموارد البشرية>

#	المسؤوليات
1	الإشراف على تنفيذ متطلبات الأمن السيبراني المتعلقة بالموارد البشرية في <اسم الجهة>.
2	التأكد من إجراء المسح الأمني للعاملين في وظائف الأمن السيبراني والوظائف التقنية ذات الصلاحيات الهامة والحساسة بالتنسيق مع الجهات المعنية.
3	تولي المسؤولية المتعلقة بدعم تطبيق سياسة الاستخدام المقبول للأصول وتطبيق العقوبات على المخالفين حسب الإجراءات المعتمدة لدى <اسم الجهة>.
4	تولي المسؤولية المتعلقة بسياسة الأمن السيبراني للموارد البشرية مما يترتب على تحديث السياسة ومراجعتها.
5	حضور اجتماعات اللجنة الإشرافية للأمن السيبراني والمشاركة بها حسب الضرورة.
6	المطالبة بالتمويل الكافي للموارد التدريبية المتعلقة بالأمن السيبراني، بما في ذلك الدورات الداخلية والدورات المتعلقة بالقطاع، والمدربين والمواد ذات الصلة.
7	إجراء تقييمات الاحتياجات التعليمية وتحديد المتطلبات المتعلقة بالأمن السيبراني.
8	التأكد من إعداد وتنفيذ أدوار ومسؤوليات وظيفية قياسية وفقاً للأدوار الوظيفية المحددة المتعلقة بالأمن السيبراني.
9	تحديد المسارات المهنية للأمن السيبراني لإتاحة الفرصة للنمو المهني والترقيات في المجالات المهنية المتعلقة بالأمن السيبراني.
10	التنسيق مع <الإدارة المعنية بالأمن السيبراني> حول المسائل المتعلقة بالأمن السيبراني التي تؤثر على <الإدارة المعنية بالموارد البشرية>.

اختر التصنيف

11	المشاركة في مراجعة استراتيجية وسياسات الأمن السيبراني وتقديم المدخلات لها.
12	التعامل مع مخالفات عدم الالتزام بسياسات الأمن السيبراني وذلك بالتنسيق مع <الإدارة المعنية بالشؤون القانونية>.

موظفو <الإدارة المعنية بالموارد البشرية>

#	المسؤوليات
1	تنفيذ متطلبات الأمن السيبراني المتعلقة بالموارد البشرية في <اسم الجهة>.
2	إجراء المسح الأمني للعاملين في وظائف الأمن السيبراني والوظائف التقنية ذات الصلاحيات الهامة والحساسة بالتنسيق مع الجهات المعنية.
3	إجراء تقييم للوعي الأمني لجميع العاملين وتحديد نقاط الضعف المتعلقة بالأمن السيبراني والعمل على معالجتها.
4	تنفيذ برنامج التوعية والتدريب بالأمن السيبراني بالتنسيق مع الإدارة المعنية بالتوعية والتدريب بالأمن السيبراني.
5	إعداد وتنفيذ أوصاف وظيفية قياسية وفقاً للأدوار الوظيفية المحددة المتعلقة بالأمن السيبراني.
6	المساعدة في تحديد المسارات المهنية للأمن السيبراني لإتاحة الفرصة للنمو المهني والترقيات في المجالات المهنية المتعلقة بالأمن السيبراني.
7	تقديم الدعم في المطالبة بالتمويل الكافي للموارد التدريبية المتعلقة بالأمن السيبراني، بما في ذلك الدورات الداخلية والدورات المتعلقة بالقطاع، والمدربين والمواد ذات الصلة.

<رئيس الإدارة المعنية بالتدقيق الداخلي>

#	المسؤوليات
1	الإشراف على المراجعة والتدقيق الدوري لبرامج ومتطلبات الأمن السيبراني وفقاً لمعايير التدقيق المتعارف عليها والمقبولة عموماً، والقوانين والتنظيمات ذات العلاقة.
2	الإشراف على تدقيق الأمن السيبراني وفقاً لشروط سياسة تدقيق ومراجعة الأمن السيبراني.
3	التأكد من المراجعة والتحديث الدوري لجميع الوثائق المتعلقة بالأمن السيبراني.

#	المسؤوليات
4	حضور اجتماعات اللجنة الإشرافية للأمن السيبراني والمشاركة بها حسب الضرورة.
5	التأكد من تحديث مخاطر الأمن السيبراني وإعادة تقييمها وفقاً لسياسة إدارة مخاطر الأمن السيبراني.
6	التأكد من مواءمة قبول المخاطر مع سياسة إدارة مخاطر الأمن السيبراني.
7	اقتراح خطّة معالجة لنتائج وملاحظات التدقيق.
8	توثيق النتائج والملاحظات والإبلاغ عنها ومناقشتها مع الإدارة المعنية.
9	تقديم نتائج وملاحظات التدقيق إلى اللجنة الإشرافية المعنية بالأمن السيبراني.
10	مناقشة الإجراءات التصحيحية مع مسؤولي نتائج التدقيق وتوثيقها.
11	الإبلاغ عن أي ضوابط غير فعّالة متعلّقة بالأمن السيبراني.
12	الإبلاغ عن عدم الالتزام بمتطلبات الأمن السيبراني.
13	التنسيق مع فريق الأمن السيبراني حول المسائل المتعلقة بالأمن السيبراني التي تؤثر على الإدارة المعنية بالتدقيق الداخلي.
14	مراجعة استراتيجية وسياسات الأمن السيبراني وتقديم المدخلات لها.

موظفو <الإدارة المعنية بالتدقيق الداخلي>

#	المسؤوليات
1	المساعدة في مراجعة وتدقيق تنفيذ ضوابط الأمن السيبراني وفقاً لمعايير التدقيق المتعارف عليها والمقبولة عموماً، والقوانين والتنظيمات ذات العلاقة.
2	تنفيذ متطلبات الأمن السيبراني المتعلقة بالتدقيق الداخلي في <اسم الجهة>.
3	المراجعة والتحديث الدوري لجميع الوثائق المتعلقة بالأمن السيبراني.
4	إجراء مراجعات للتأكّد من تحديث مخاطر الأمن السيبراني وإعادة تقييمها وفقاً لسياسة إدارة مخاطر الأمن السيبراني.
5	إجراء مراجعات للتأكد من مواءمة قبول المخاطرمع سياسة إدارة مخاطر الأمن السيبراني.

#	المسؤوليات
6	إجراء مراجعات وإبلاغ رئيس التدقيق الداخلي بعدم الالتزام بمتطلبات الأمن السيبراني.
7	تنفيذ عملية تدقيق الأمن السيبراني وفقاً لشروط سياسة تدقيق ومراجعة الأمن السيبراني.
8	تحليل الضوابط الفعالة للأمن السيبراني، وتقديم التوصيات لرئيس التدقيق الداخلي بشأنها.
9	اقتراح الإجراءات التصحيحية على رئيس التدقيق الداخلي وفقاً لنتائج وملاحظات التدقيق.
10	المساعدة في اقتراح خطّة معالجة لنتائج وملاحظات التدقيق.
11	المساعدة في التنسيق مع فريق الأمن السيبراني حول المسائل المتعلقة بالأمن السيبراني التي تؤثر على الإدارة المعنية بالتدقيق الداخلي.

<الإدارة المعنية بالشؤون القانونية>

#	المسؤوليات
1	حصر المتطلبات التنظيمية والتشريعية الوطنية ذات العلاقة بالأمن السيبراني، والاتفاقيات والالتزامات الدولية المعتمدة محلياً التي تتضمن متطلبات خاصة بالأمن السيبراني تنطبق على <اسم الجهة>.
2	ترجمة ضوابط الأمن السيبراني وتنظيماته وسياساته ومعاييره وإجراءاته، وجعلها ملزمة قانونياً.
3	التأكد من أن الشروط والأحكام وبنود المحافظة على سرية المعلومات (Non-Disclosure Clauses) ملزمة للموظفين وللأطراف الخارجية من أجل حماية الأصول المعلوماتية والتقنية لـ<اسم الجهة>.
4	الإشراف على تنفيذ متطلبات الأمن السيبراني المتعلقة بالشؤون القانونية في <اسم الجهة>.
5	حضور اجتماعات اللجنة الإشرافية للأمن السيبراني والمشاركة بها حسب الضرورة.
6	تقييم فعالية قوانين وتنظيمات الأمن السيبراني.
7	مراجعة سياسة أمن الأطراف الخارجية المعتمدة في <اسم الجهة> وفقاً للمتطلّبات القانونية ذات العلاقة.
8	العمل مع <الإدارة المعنية بالأمن السيبراني> حول المسائل المتعلقة بالأمن السيبراني التي تؤثر على الإدارة المعنية بالشؤون القانونية.

#	المسؤوليات
9	تقديم الدعم لحوادث الأمن السيبراني عند الحاجة.

موظفو <الإدارة المعنية بالشؤون القانونية>

#	المسؤوليات
1	المساعدة في تفسير قوانين الأمن السيبراني وتنظيماته وسياساته ومعاييره وإجراءاته وتطبيقها على مسائل محددة.
2	تنفيذ متطلبات الأمن السيبراني المتعلقة بالشؤون القانونية في <اسم الجهة>.
3	المساعدة في تقييم فعالية قوانين وتنظيمات الأمن السيبراني.

جميع العاملين

#	المسؤوليات
1	التعامل مع البيانات والمعلومات حسب مستوى تصنيفها.
2	تلافي انتهاك حقوق أي شخص أو شركة محمية بحقوق النشر أو براءة الاختراع أو أي ملكية فكرية أخرى أو قوانين أو لوائح مماثلة.
3	الالتزام بسياسات وإجراءات الأمن السيبراني.
4	الالتزام بمتطلبات الأمن السيبراني المتعلقة بحماية أجهزة المستخدمين.
5	الالتزام بمتطلبات الأمن السيبراني المتعلقة باستخدام الإنترنت والبرمجيات.
6	الالتزام بمتطلبات الأمن السيبراني المتعلقة بالبريد الإلكتروني.
7	الالتزام بالمتطلبات المتعلقة بنظم وتقنيات حماية الأمن السيبراني.
8	استخدام جميع الأصول المعلوماتية والتقنية الخاصة بـ<اسم الجهة> لأغراض العمل فقط وحسب سياسة الاستخدام المقبول للأصول المعتمدة في <اسم الجهة>.
9	الحصول على التصريح المطلوب من <الإدارة المعنية في الجهة> أو صاحب الصلاحية في <اسم الجهة> قبل استضافة الزوار في المواقع الحساسة المحددة في <اسم الجهة>.

اختر التصنيف

10	الإبلاغ عن حوادث الأمن السيبراني.
11	الالتزام بسياسة الاستخدام المقبول.

الأدوار والمسؤوليات

1- **راعي ومالك الوثيقة:** <رئيس الإدارة المعنية بالأمن السيبراني>.

2- **مراجعة الوثيقة وتحديثها:** <الإدارة المعنية بالأمن السيبراني>.

3- **تنفيذ الوثيقة وتطبيقها:** <الإدارة المعنية بالأمن السيبراني> و<الإدارة المعنية بالموارد البشرية>.