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

اختر التصنيف

التاريخ: اضغط هنا لإضافة تاريخ

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

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

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

إخلاء المسؤولية

طُور هذا النموذج عن طريق الهيئة الوطنية للأمن السيبراني كمثال توضيحي يمكن استخدامه كدليل ومرجع للجهات. يجب أن يتم تعديل هذا النموذج ومواءمته مع أعمال <اسم الجهة> والمتطلبات التشريعية والتنظيمية ذات العلاقة. كما يجب أن يُعتمد هذا النموذج من قبل رئيس الجهة أو من يقوم/تقوم بتفويضه. وتخلي الهيئة مسؤوليتها من استخدام هذا النموذج كما هو، وتؤكد على أن هذا النموذج ما هو إلا مثال توضيحي.

اعتماد الوثيقة

الدور	المسمى الوظيفي	الاسم	التاريخ	التوقيع
اختر الدور	<أدخل المسمى الوظيفي>	<أدخل الاسم الكامل للموظف>	اضغط هنا لإضافة تاريخ	<أدخل التوقيع>

نسخ الوثيقة

النسخة	التاريخ	عُدلَ بواسطة	أسباب التعديل
<أدخل رقم النسخة>	اضغط هنا لإضافة تاريخ	<أدخل الاسم الكامل للموظف>	<أدخل وصف التعديل>

جدول المراجعة

معدل المراجعة	التاريخ لأخر مراجعة	تاريخ المراجعة القادمة
مره واحدة كل سنة	اضغط هنا لإضافة تاريخ	اضغط هنا لإضافة تاريخ

قائمة المحتويات

مقدمة 0

الغرض 0

نطاق الوثيقة 0

جدول فصل مسؤوليات المكونات الفرعية للضوابط الأساسية للأمن السيبراني (ECC-١:٢٠١٨) 0

الأدوار والمسؤوليات المتعلقة بالأمن السيبراني ٧

<صاحب الصلاحية> ٧

أعضاء اللجنة الإشرافية للأمن السيبراني ٧

<رئيس الإدارة المعنية بالأمن السيبراني> ٩

الأدوار والمسؤوليات الخاصة <بالإدارة المعنية بالأمن السيبراني> ١١

<رئيس مكتب إدارة البيانات> ٥١

موظفو <مكتب إدارة البيانات> ٥٢

<رئيس الإدارة المعنية بتقنية المعلومات> ٥٧

موظفو <الإدارة المعنية بتقنية المعلومات> ٥٨

الأدوار والمسؤوليات الخاصة ب<أمن تقنية المعلومات> ٥٩

<مسؤول تطوير التطبيقات> ٦٨

المعنيون بتطوير التطبيقات ٦٩

<مسؤول عمليات تقنية المعلومات> ٧٠

المعنيون بعمليات تقنية المعلومات ٧١

<رئيس الإدارة المعنية بالموارد البشرية> ٧٢

موظفو <الإدارة المعنية بالموارد البشرية> ٧٣

<رئيس الإدارة المعنية بالتدقيق الداخلي> ٧٤

موظفو <الإدارة المعنية بالتدقيق الداخلي> ٧٥

<الإدارة المعنية بالشؤون القانونية> ٧٥

موظفو <الإدارة المعنية بالشؤون القانونية> ٧٦

جميع العاملين في <اسم الجهة> ٧٦

جدول فصل مهام إدارة وتشغيل الأنظمة والأدوات المتعلقة بالأمن السيبراني ٧٨

الأدوار والمسؤوليات ٧٩

التحديث والمراجعة.....٧٩
الالتزام بالوثيقة.....٧٩
جدول المراجع.....٧٩

مقدمة

تم تطوير هذه الوثيقة لتحديد الأدوار والمسؤوليات اللازمة لتلبية متطلبات 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>.

الغرض

تهدف هذه الوثيقة إلى تحديد أدوار ومسؤوليات الأمن السيبراني في <اسم الجهة> وذلك لتحقيق الغرض الأساسي من الوثيقة وهو التأكد من أن جميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني في الجهة على دراية بمسؤولياتهم في تطبيق برامج ومتطلبات الأمن السيبراني في <اسم الجهة> والجهات التابعة لها. هذه الأدوار والمسؤوليات تمت موائمتها مع الإطار السعودي لكوادر الأمن السيبراني الصادر من الهيئة الوطنية للأمن السيبراني (SCyWF – ١:٢٠٢٠).

نطاق الوثيقة

تطبق هذه الوثيقة على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

جدول فصل مسؤوليات المكونات الفرعية للضوابط الأساسية للأمن السيبراني (ECC-١:٢٠١٨)

إن جوانب الحوكمة والمخاطر والالتزام لجميع المكونات الفرعية تعتبر مسؤولية <الإدارة المعنية بالأمن السيبراني>، أما فيما يتعلق بالتطبيق يختلف من مكون فرعي إلى آخر حيث تم توضيح مسؤولية التطبيق للمكونات الفرعية للأمن السيبراني في الجدول أدناه:

رقم المكون الفرعي من الضوابط الأساسية	المكون الفرعي للأمن السيبراني	الإدارة المسؤولة عن التطبيق
١-٥	إدارة مخاطر الأمن السيبراني	<الإدارة المعنية بالأمن السيبراني> (قسم الحوكمة والمخاطر والالتزام)
١-٦	الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية	<الإدارة المعنية بالأمن السيبراني> (قسم الحوكمة والمخاطر والالتزام)
١-٨	المراجعة والتدقيق الدوري للأمن السيبراني	<الإدارة المعنية بالأمن السيبراني> (قسم الحوكمة والمخاطر والالتزام)
١-٩	الأمن السيبراني المتعلق بالموارد البشرية	<الإدارة المعنية بالموارد البشرية>
١-١٠	برنامج التوعية والتدريب بالأمن السيبراني	<الإدارة المعنية بالأمن السيبراني> و <الإدارة المعنية بالموارد البشرية>
٢-١	إدارة الأصول	<الإدارة المعنية بتقنية المعلومات> و <الإدارة المعنية بالأمن والسلامة وإدارة المرافق>

رقم المكون الفرعي من الضوابط الأساسية	المكون الفرعي للأمن السيبراني	الإدارة المسؤولة عن التطبيق
٢-٢	إدارة هويات الدخول والصلاحيات	<الإدارة المعنية بتقنية المعلومات> و <الإدارة المعنية بالأمن والسلامة وإدارة المرافق>
٢-٣	حماية الأنظمة وأجهزة معالجة المعلومات	<الإدارة المعنية بتقنية المعلومات>
٢-٤	حماية البريد الالكتروني	<الإدارة المعنية بتقنية المعلومات>
٢-٥	إدارة أمن الشبكات	<الإدارة المعنية بتقنية المعلومات>
٢-٦	أمن الأجهزة المحمولة	<الإدارة المعنية بتقنية المعلومات>
٢-٧	حماية البيانات والمعلومات	<الإدارة المعنية بتقنية المعلومات> و <مكتب إدارة البيانات>
٢-٨	التشفير	<الإدارة المعنية بتقنية المعلومات>
٢-٩	إدارة النسخ الاحتياطية	<الإدارة المعنية بتقنية المعلومات>
٢-١٠	إدارة الثغرات	<الإدارة المعنية بالأمن السيبراني> (قسم عمليات الأمن السيبراني) و <الإدارة المعنية بتقنية المعلومات>
٢-١١	اختبار الاختراق	<الإدارة المعنية بالأمن السيبراني> (قسم عمليات الأمن السيبراني)
٢-١٢	إدارة سجلات الأحداث ومراقبة الأمن السيبراني	<الإدارة المعنية بالأمن السيبراني> (قسم عمليات الأمن السيبراني)
٢-١٣	إدارة حوادث وتهديدات الأمن السيبراني	<الإدارة المعنية بالأمن السيبراني> (قسم عمليات الأمن السيبراني)
٢-١٤	الأمن المادي	<الإدارة المعنية بالأمن والسلامة وإدارة المرافق>
٢-١٥	حماية تطبيقات الويب	<الإدارة المعنية بتقنية المعلومات> و <الإدارة المعنية بالأمن السيبراني>
٣-١	جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال	<الإدارة المعنية بالأمن السيبراني> و <الإدارة المعنية باستمرارية الأعمال>
٤-١	الأمن السيبراني المتعلق بالأطراف الخارجية	<الإدارة المعنية بالأمن السيبراني> و <الإدارة المعنية بالمشتريات والأطراف الخارجية>
٤-٢	الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة	<الإدارة المعنية بتقنية المعلومات> و <الإدارة المعنية بالأمن السيبراني> و <الإدارة المعنية بالمشتريات والأطراف الخارجية>
٥-١	حماية أجهزة وأنظمة التحكم الصناعي	<الإدارة المعنية بالأمن السيبراني> و <الإدارة المعنية بأنظمة التحكم الصناعي>

الأدوار والمسؤوليات المتعلقة بالأمن السيبراني

<صاحب الصلاحية>

#	المسؤوليات
١	تأسيس <الإدارة المعنية بالأمن السيبراني> وضمان استقلاليتها لعدم تضارب المصالح، وتعيين <رئيس الإدارة المعنية بالأمن السيبراني> وأن يكون سعودي الجنسية.
٢	تأسيس اللجنة الإشرافية للأمن السيبراني.
٣	الموافقة على وثيقة اللجنة الإشرافية للأمن السيبراني.
٤	تخصيص الميزانية الكافية لمتطلبات الأمن السيبراني بما في ذلك ميزانية الموارد البشرية.
٥	اعتماد استراتيجية الأمن السيبراني بعد رفعها للّجنة الإشرافية للأمن السيبراني.
٦	اعتماد سياسات وإجراءات الأمن السيبراني من قبل صاحب الصلاحية بعد رفعها للّجنة الإشرافية للأمن السيبراني.
٧	اعتماد وثيقة حوكمة الأمن السيبراني والهيكل التنظيمي والأدوار والمسؤوليات الخاصة بالأمن السيبراني بعد رفعهما للّجنة الإشرافية للأمن السيبراني في <اسم الجهة> من قبل صاحب الصلاحية.
٨	اعتماد وثيقة إدارة المخاطر السيبرانية بعد رفعهما للّجنة الإشرافية للأمن السيبراني.
٩	الاطلاع على تقارير حالة الأمن السيبراني دوريًا، وتوفير الدعم المطلوب.

أعضاء اللجنة الإشرافية للأمن السيبراني

#	المسؤوليات
١	متابعة المتطلبات الأمنية وفقًا للوثيقة المنظمة للجنة الإشرافية للأمن السيبراني في <اسم الجهة>.
٢	ترسيخ مبادئ المساءلة والمسؤولية والصلاحية من خلال تحديد الأدوار والمسؤوليات بهدف حماية الأصول المعلوماتية والتقنية الخاصة ب<اسم الجهة>.
٣	التأكد من وجود وثيقة معتمدة توضح منهجية إدارة وتقييم المخاطر السيبرانية ومستوى المخاطر المقبول (Risk Appetite) لدى <اسم الجهة>، ومراجعتها بشكل مستمر أو عند حدوث أي تغيير جوهري في مستوى المخاطر المقبول.

#	المسؤوليات
٤	الموافقة على إجراءات إدارة مخاطر الأمن السيبراني ودعمها ومراقبتها.
٥	الموافقة على وثيقة الأمن السيبراني ودعمها ومراقبتها.
٦	مراجعة استراتيجية الأمن السيبراني لضمان توافقها مع الأهداف الاستراتيجية ل<اسم الجهة> قبل اعتمادها من صاحب الصلاحية.
٧	اعتماد خطة العمل الخاصة بتنفيذ استراتيجية الأمن السيبراني ودعمها ومراقبتها.
٨	دعم ومراقبة تطبيق سياسات الأمن السيبراني.
٩	اعتماد مبادرات ومشاريع الأمن السيبراني (مثل: برنامج التوعية بالأمن السيبراني، وحماية البيانات والمعلومات، وغيرها) ودعمها ومراقبتها.
١٠	الموافقة على مؤشرات الأداء (Key Performance Indicators "KPIs") ومتابعتها، والتأكد من فعاليتها لأعمال <الإدارة المعنية بالأمن السيبراني> والعمل على رفع مستوى الأداء.
١١	متابعة إدارة حوادث الأمن السيبراني ودعمها.
١٢	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.
١٣	مراجعة التقارير الخاصة بمخاطر الأمن السيبراني ومتابعة معالجتها وتقديم الدعم اللازم لمعالجتها أو العمل على تقليلها.
١٤	مراجعة التقارير الأمنية الخاصة بحوادث الأمن السيبراني وتقديم التوصيات بشأنها.
١٥	مراجعة طلبات الاستثناءات الخاصة بالأمن السيبراني وتقديم التوصيات بشأنها.
١٦	متابعة تقارير حالة حزم التحديثات والإصلاحات الأمنية، وتقييم الثغرات الأمنية على جميع الأصول التقنية والمعلوماتية والتأكد من معالجتها.
١٧	مراجعة نتائج تدقيق الأمن السيبراني الداخلي والخارجي، والتأكد من وجود خطة مناسبة لمعالجة الملاحظات المكتشفة ومتابعتها وتقديم الدعم اللازم لمعالجتها.
١٨	رفع التقارير الدورية عن حالة الأمن السيبراني والدعم المطلوب لصاحب الصلاحية.

#	المسؤوليات
١٩	مراجعة حالة الالتزام بالمتطلبات الداخلية للجهة والمتطلبات التشريعية الصادرة من الهيئة الوطنية للأمن السيبراني.

<رئيس الإدارة المعنية بالأمن السيبراني>

#	المسؤوليات
١	التواصل الفعّال مع الإدارة العليا بشأن جوانب الأمن السيبراني، والتأكد من أن متطلبات الأمن السيبراني لتقنية المعلومات تتوافق مع استراتيجية الأمن السيبراني في الجهة.
٢	التعاون مع أصحاب المصلحة لضمان تلبية برامج استمرارية الأعمال والتعافي من الكوارث لمتطلبات الجهة.
٣	إدارة معالجة الثغرات بفعالية.
٤	الإشراف على الموظفين القائمين على مهام الأمن السيبراني وإسناد الأعمال إليهم بفاعلية.
٥	تخصيص الموارد اللازمة لأدوار الأمن السيبراني.
٦	رفع الوعي بالسياسة والاستراتيجية السيبرانية بين مدراء الإدارات في الجهة.
٧	العمل مع أصحاب المصلحة لتطوير سياسات الأمن السيبراني والوثائق المصاحبة بما يتوافق مع استراتيجية الأمن السيبراني للجهة.
٨	تطوير/ تأسيس استراتيجية الأمن السيبراني.
٩	ضمان موافقة استراتيجية الأمن السيبراني للجهة مع استراتيجيتها للأعمال.
١٠	ضمان إجراء تقييم لمخاطر الأمن السيبراني.
١١	ضمان تقديم الدعم لتطبيق السياسات والعمليات والإجراءات ذات العلاقة بالخصوصية والأمن السيبراني.
١٢	ضمان وضع الضوابط الملائمة للحد من مخاطر الأمن السيبراني بفاعلية ومعالجة مخاوف الخصوصية خلال عملية تقييم المخاطر.
١٣	ضمان تقديم الدعم لتنفيذ وحفظ برنامج إدارة مخاطر الأمن السيبراني.

#	المسؤوليات
١٤	ضمان عكس مبادئ سليمة للأمن السيبراني على رسالة الجهة ورؤيتها وأهدافها.
١٥	حيازة الموارد اللازمة لتطوير وتطبيق عمليات فعّالة تلبي الأهداف الأمنية والمعلوماتية الاستراتيجية.
١٦	فهم الحالة الأمنية لمعلومات الجهة والتعبير عنها خلال عمليات التمحيص القانوني والتنظيمي.
١٧	دعم الأمن السيبراني وإبراز قيمته لدى أصحاب المصلحة في الجهة.
١٨	التواصل بفاعلية مع الأطراف الخارجية عند وقوع حادث أمن سيبراني.
١٩	ضمان مراجعة فاعلية ضوابط الأمن السيبراني للجهة ومواءمتها لأهدافها الاستراتيجية.
٢٠	إدارة التقييم والصيانة الدورية لسياسات الأمن السيبراني بالجهة والوثائق ذات العلاقة.
٢١	التأكد من اتخاذ الإجراءات الملائمة لمعالجة الخطر عند وقوع حادثة متعلق بالأمن السيبراني.
٢٢	دعم القضايا الأمنية لدى الإدارة العليا، والتأكد من شمول الأمن السيبراني ضمن الأهداف الاستراتيجية.
٢٣	التأكد من معالجة استراتيجية الأمن السيبراني للجهة بفعالية من خلال سياسات الأمن السيبراني والوثائق ذات الصلة.
٢٤	التأكد من تحديد متطلبات الأمن السيبراني لكافة أنظمة تقنية المعلومات.
٢٥	تطوير سياسات الأمن السيبراني المناسبة والوثائق ذات العلاقة وحفظها لضمان حماية البنية التحتية الحساسة للجهة بشكل ملائم.
٢٦	التعاون مع أصحاب المصلحة في الجهة والأطراف الآخرين عند تحديد المتطلبات المستقبلية للخطة الاستراتيجية للأمن السيبراني.
٢٧	تحديد وتعيين الموارد الخبيرة الملائمة للقيام بأنشطة الأمن السيبراني في الجهة.
٢٨	حضور الفعاليات الدولية للأمن السيبراني وإلقاء الكلمات فيها عند الحاجة.
٢٩	حيازة الموارد الملائمة لتنفيذ وحفظ جوانب الأمن السيبراني لخطة استمرارية أعمال فعالة.
٣٠	تطوير وحفظ خطط استراتيجية للأمن السيبراني تتوافق مع خطة الأعمال الاستراتيجية للجهة.
٣١	التأكد من أن متطلبات الأمن السيبراني لتقنية المعلومات تتوافق مع استراتيجية الأمن السيبراني في الجهة.

#	المسؤوليات
٣٢	إدارة الجوانب المالية للأمن السيبراني شاملة إعداد الميزانية وتوفير الموارد.
٣٣	التأكد من فاعلية إيصال المعلومات التي تخص تهديدات الأمن السيبراني وأساليب معالجتها إلى الأطراف الأخرى المهتمة.

الأدوار والمسؤوليات الخاصة <بالإدارة المعنية بالأمن السيبراني>

مصمم معمارية الأمن السيبراني (Cybersecurity Architect)

#	المسؤوليات
١	إجراء مراجعات الأمن السيبراني، وتحديد الفجوات في المعمارية الأمنية، من أجل إصدار خطط لإدارة المخاطر السيبرانية.
٢	توفير مدخلات لإطار إدارة المخاطر والوثائق ذات الصلة.
٣	تنفيذ عمليات آمنة لإدارة الإعدادات.
٤	تحديد وظائف الأعمال الحيوية وتصنيف أولوياتها بالتعاون مع أصحاب المصلحة بالجهة.
٥	تقديم استشارات بشأن تكاليف المشاريع، ومفاهيم التصميم التابعة لها، أو التغييرات على تصاميمها.
٦	تقديم المشورة بشأن المتطلبات الأمنية المطلوب إدراجها في وثائق المشتريات.
٧	تحليل المعمارية المرشحة، وتخصيص الخدمات الأمنية واختيار الآليات الأمنية.
٨	تعريف السياق الأمني للنُظم، ومفهوم العمليات واحتياجاتها المبدئية، وفقًا لسياسات الأمن السيبراني المطبقة.
٩	تحرير المواصفات الوظيفية التفصيلية التي توثق عملية تطوير المعمارية.
١٠	تحليل احتياجات المستخدم ومتطلباته لتخطيط المعمارية.
١١	تطوير المعمارية المؤسسية أو مكونات النظام المطلوبة لتلبية احتياجات المستخدم.
١٢	توثيق وتحديث كل أنشطة التعريف والمعمارية، حسب الضرورة.

#	المسؤوليات
١٣	تحديد ضوابط الأمن لنظم المعلومات والشبكات، مع توثيقها على نحو ملائم.
١٤	تقييم وتصميم وظائف إدارة الأمن السيبراني.
١٥	تعريف لمستويات التوافر المناسبة لوظائف النظم الحرجة ومتطلبات عمليات التعافي من الكوارث والاستمرارية لتقديمها.
١٦	تحديد وترتيب أولويات قدرات النُظم أو وظائف الأعمال اللازمة لاستعادة النظام جزئيًا أو كليًا بعد وقوع عطل كارثي.
١٧	تطوير ودمج تصاميم الأمن السيبراني للنُظم والشبكات والتي لها متطلبات أمن متعددة المستويات.
١٨	توثيق ومعالجة متطلبات الجهة للأمن السيبراني في المعمارية وهندسة النظم في كافة مراحل عمليات الشراء والاستحواذ.
١٩	ضمان اتساق النُظم والمعمارية التي تمت حيازتها أو تطويرها مع إرشادات الجهة لمعمارية الأمن السيبراني.
٢٠	ترجمة القدرات المقترحة إلى متطلبات تقنية.
٢١	العمل مع أعضاء فريق التطوير المرن لتسريع إعداد نماذج أولية ودراسات الجدوى وتقييم التقنيات الحديثة.
٢٢	تصميم نُظم وحلول لدعم نجاح "حلول إثبات المبدأ" والمشاريع التجريبية في مجالات التقنيات الناشئة.
٢٣	قراءة وتفسير المخططات والمواصفات والرسومات والتصاميم الأولية والرسومات البيانية التخطيطية ذات العلاقة بالأنظمة والشبكات.
٢٤	تحديد وتوثيق الضوابط الأمنية للأنظمة والشبكات.
٢٥	تحديد وتوثيق أثر تنفيذ نظام جديد أو واجهات اتصال جديدة بين النُظم على الوضع الأمني للبيئة الحالية.
٢٦	تقديم التوصيات بخصوص الضوابط الأمنية ذات الكفاءة المالية لمعالجة المخاطر المكتشفة عن طريق الاختبار والمراجعة.

أخصائي الحوسبة السحابية الآمنة (Secure Cloud Specialist)

#	المسؤوليات
١	تطوير عناصر المعمارية الأمنية للحد من التهديدات عند نشوئها.
٢	تقديم حلول سحابية آمنة إلى فرق التطوير، وضمان أمان السحب المنقولة، وأمان عملية تطوير التطبيقات السحابية.
٣	العمل ضمن فرق متعددة التخصصات كخبير متخصص في معايير معمارية الأمن السحابي ومنهجياتها.
٤	تقييم التصاميم الأمنية ومعماريتها، وتحديد مدى كفايتها.
٥	تطوير وتنفيذ استراتيجية سحابية آمنة بالتلازم مع أعمال المعمارية المؤسسية.
٦	تطوير وتنفيذ أنماط آمنة لاستهلاك فرق التقنية للخدمات السحابية.
٧	بناء حلول لتحديد بيانات الجهة المتواجدة بداخل البيئات السحابية.
٨	توفير الخبرة المتخصصة لتطوير وهندسة الجيل القادم من الأمن السيبراني.
٩	بناء الضوابط الأمنية حيث يلزم لمراقبة وحماية المعلومات المخزنة في البيئات السحابية على نحو ملائم.
١٠	تقديم المشورة المتخصصة في أمن معمارية الحوسبة السحابية شاملا الشبكات، والتخزين، وقواعد البيانات، والتوفير والإدارة.

مقيم البرمجيات الآمنة (Secure Software Assessor)

#	المسؤوليات
١	تحليل المخاطر كلما خضع أي برنامج أو نظام لتغيير جوهري.
٢	تحليل نتائج التمارين وبيئة النظام للتخطيط وللتوصية بتعديلات وتسويات.
٣	الإشراف على الموظفين القائمين على مهام الأمن السيبراني وإسناد الأعمال إليهم بفاعلية.
٤	تطبيق معايير الأمن للبرمجة والاختبار.
٥	توثيق الشفرات البرمجية الآمنة.
٦	دمج الأمن السيبراني في عملية المتطلبات عن طريق تعريف الضوابط الأمنية وتوثيقها.

#	المسؤوليات
٧	إصدار نموذج التهديدات استنادًا إلى المقابلات مع العملاء وتحديد متطلباتهم.
٨	تقييم مواطن الارتباط بين العتاد والبرامج من خلال التشاور مع الكوادر الهندسية.
٩	الإفادة بمعلومات لمهام إعداد الأجهزة من خلال تقييم القيود المالية والقيود الأمنية.
١٠	تطبيق المنهجيات لإصلاح الأخطاء البرمجية الشائعة ذات التبعات الأمنية لضمان تطوير برمجيات آمنة.
١١	ضمان تضمين الأمن السيبراني بداخل عمليات تطوير البرامج، وحفظها، وإخراجها من الخدمة.
١٢	إجراء اختبارات مدمجة لضمان جودة وظائف الأنظمة الأمنية وصمودها.
١٣	معالجة التبعات الأمنية في مرحلة قبول البرمجيات.
١٤	تخزين البيانات واسترجاعها ومعالجتها لتحليل قدرات النظام ومتطلباته.
١٥	ترجمة المتطلبات الأمنية إلى عناصر تصميم التطبيق، بما في ذلك توثيق عناصر الأجزاء المعرضة للهجوم في البرمجيات وتصميم نماذج للتهديدات وتحديد أي ضوابط أمنية خاصة.
١٦	ضمان إجراء اختبارات الاختراق عند الحاجة للتطبيقات الجديدة أو المحدَّثة.
١٧	استشارة العملاء بخصوص تصميم أنظمة الأمن السيبراني وصيانتها.
١٨	توجيه أعمال البرمجة لتطبيقات الأمن السيبراني وأعمال تطوير مستنداتها التوثيقية.
١٩	إجراء أعمال التحليل لتقديم معلومات إلى أصحاب المصلحة بما يدعم تطوير تطبيقات أمنية أو تعديلها.
٢٠	تحليل الاحتياجات الأمنية ومتطلبات البرمجيات، لتحديد جدوى التصميم ضمن الحدود الزمنية وقيود التكلفة والالتزامات الأمنية.
٢١	التشغيل التجريبي للبرامج وتطبيقات البرمجيات، لضمان إنتاج المعلومات المرغوبة، وضمان سلامة التعليمات والمستويات الأمنية.
٢٢	تطوير إجراءات اختبار البرمجيات الآمنة والمصادقة عليها.
٢٣	تطوير إجراءات اختبارات النظم ومصادقتها، شاملا البرمجة والتوثيق.
٢٤	إجراء اختبارات ومراجعات وتقييمات البرامج الآمنة لتحديد مواطن الخلل المحتملة في الشفرات البرمجية ومعالجة الثغرات.

#	المسؤوليات
٢٥	تحديد وتوثيق حزم تحديثات الإصلاح للبرمجيات أو نطاق الإصدارات الذي سينشأ عنه ثغرات بالبرامج.
٢٦	تحديد المشكلات الأمنية المتعلقة بالتشغيل المستقر للبرامج وإدارتها وعمل الإجراءات الأمنية اللازمة عندما يصل منتج معين لنهاية دورة حياته.

باحث الأمن السيبراني (Cybersecurity Researcher)

#	المسؤوليات
١	البحث في التقنيات المعاصرة لفهم قدرات الدفاع السيبراني المطلوبة من قبل النظم أو الشبكة.
٢	تحديد وتطوير أدوات الهندسة العكسية لتعزيز القدرات والكشف عن الثغرات.
٣	تطوير قدرات إدارة البيانات الآمنة لدعم القوى العاملة المتنقلة.
٤	مراجعة برامج التنقيب عن البيانات ومستودعات البيانات وعملياتهما ومتطلباتهما، والتحقق من مصداقيتها.
٥	تحديد استراتيجيات القدرات السيبرانية لتطوير الأجهزة والبرمجيات المخصصة حسب متطلبات الجهة.
٦	التعاون مع أصحاب المصلحة لتحديد الحلول التقنية المناسبة.
٧	تصميم وتطوير أدوات وتقنيات الأمن السيبراني الجديدة.
٨	تقييم الثغرات في بنية الشبكات.
٩	اتباع معايير وعمليات دورة حياة هندسة البرمجيات والنُظم عند تطوير نظم وحلول الأمن السيبراني.
١٠	استكشاف أخطاء التصاميم في نماذج الجدوى الأولية، ومعالجة المشاكل عبر مراحل تصميم المنتجات، وتطويرها، والإعداد لإطلاقها.
١١	إيجاد فرص تطوير القدرات الجديدة لمعالجة الثغرات.
١٢	بحث وتقييم التقنيات والمعايير المتوفرة، لتلبية متطلبات العملاء.

#	المسؤوليات
١٣	مراجعة المتطلبات التشغيلية للبحث والتطوير والاستحواذ للقدرات السيبرانية، واعتمادها، وترتيب أولوياتها، وتقديمها.

أخصائي علم البيانات للأمن السيبراني (Cybersecurity Data Science Specialist)

#	المسؤوليات
١	جمع المقاييس وبيانات التوجهات.
٢	تقديم المعلومات التقنية للجماهير التقنية وغير التقنية.
٣	عرض البيانات بصيغ مبتكرة.
٤	تحليل وتحديد متطلبات البيانات ومواصفاتها.
٥	التحليل والتخطيط للتغييرات المتوقعة في متطلبات سعة البيانات.
٦	تطوير معايير البيانات وسياساتها وإجراءاتها.
٧	إدارة تجميع البيانات، وفهرستها، والتخزين المؤقت لها، وتوزيعها واسترجاعها.
٨	توفير تدفق منظم للمعلومات ذات الصلة (عن طريق البوابات الإلكترونية على الشبكة العنكبوتية أو الوسائل الأخرى) حسب متطلبات الرسالة.
٩	تقديم توصيات بشأن التقنيات والمعمارية الجديدة لقواعد البيانات.
١٠	تحليل مصادر البيانات لتقديم توصيات قابلة للتنفيذ.
١١	تقييم صلاحية البيانات المصدرية والنتائج اللاحقة.
١٢	اختبار الفرضيات باستخدام العمليات الإحصائية.
١٣	التشاور مع محللي النُظم والمهندسين والمبرمجين وغيرهم لتصميم تطبيقات الأمن السيبراني.
١٤	تطوير منهجيات جمع البيانات وإتاحتها.
١٥	تطوير الرؤى الاستراتيجية من مجموعات البيانات الكبيرة.
١٦	برمجة خوارزميات مخصصة.

#	المسؤوليات
١٧	تقديم توصيات قابلة للتطبيق لأصحاب المصلحة، استنادًا إلى تحليل البيانات والنتائج.
١٨	استخدام المستندات أو الموارد التقنية لتنفيذ طريقة رياضية جديدة أو طريقة تعتمد على علوم البيانات أو علوم الحاسوب.
١٩	التخصيص الفعّال لسعة التخزين في تصميم نُظم إدارة البيانات.
٢٠	قراءة النصوص البرمجية البسيطة وتفسيرها وتحريرها وتعديلها وتنفيذها لأداء المهام.
٢١	استخدام لغات برمجة مختلفة لكتابة الشفرات البرمجية ولفتح الملفات، ولقراءتها، ولكتابة المخرجات في ملفات مختلفة.
٢٢	استخدام لغات مفتوحة المصدر.
٢٣	تطوير وتنفيذ برامج استخراج البيانات وبرامج مستودعات البيانات.
٢٤	استخدام التقنيات الكمية.

مدير الأمن السيبراني (Cybersecurity Manager)

#	المسؤوليات
١	التواصل الفعّال مع الإدارة العليا بشأن مخاطر الأمن السيبراني.
٢	التواصل الفعّال مع الإدارة العليا بشأن الجوانب المالية للأمن السيبراني.
٣	التعاون مع أصحاب المصلحة لضمان تلبية برامج استمرارية الأعمال والتعافي من الكوارث لمتطلبات الجهة.
٤	التأكد من توافق قدرات الاكتشاف والحماية السيبرانية مع استراتيجية وسياسات الأمن السيبراني للجهة، ومع المستندات الأخرى ذات العلاقة.
٥	التأكد من أن القرارات المتخذة بشأن الأمن السيبراني تستند على المبادئ الأساسية لإدارة المخاطر.
٦	التعرف على أنماط عدم الالتزام بسياسات الأمن السيبراني والوثائق ذات العلاقة بهدف تعريف طرق لتحسينها.

#	المسؤوليات
٧	تتبع نتائج وتوصيات التدقيق لضمان اتخاذ إجراءات معالجة ملائمة.
٨	إدارة معالجة الثغرات بفعالية.
٩	ضمان مراعاة متطلبات الجهة للأمن السيبراني في عمليات الدمج والاستحواذ والاستعانة بالموارد الخارجية وغيرها من العمليات التي تشمل طرفا ثالثاً.
١٠	المراجعة الدورية لاستراتيجية الأمن السيبراني وسياساته والوثائق ذات العلاقة للمحافظة على الالتزام بالقوانين والأنظمة المعمول بها.
١١	البقاء على معرفة بتهديدات الأمن السيبراني على الجهة.
١٢	ضمان عكس مبادئ سليمة للأمن السيبراني على رسالة الجهة ورؤيتها وأهدافها.
١٣	حيازة الموارد اللازمة لتطوير وتطبيق عمليات فعّالة تلبي الأهداف الأمنية والمعلوماتية الاستراتيجية.
١٤	ضمان جمع وحفظ البيانات اللازمة لتلبية المتطلبات المحددة لتقارير الأمن السيبراني.
١٥	دعم الأمن السيبراني وإبراز قيمته لدى أصحاب المصلحة في الجهة.
١٦	ضمان تقييم أنشطة التحسينات الأمنية، وتنفيذها ومراجعتها حسب الحاجة.
١٧	ضمان تنسيق حملات تفتيش الأمن السيبراني في البيئة الشبكية، وأعمال الاختبارات والمراجعات.
١٨	ضمان إدراج متطلبات الأمن السيبراني في كافة عمليات التخطيط لاستمرارية الأعمال وتلافي الكوارث.
١٩	ضمان توافق تصاميم معمارية الأمن السيبراني مع استراتيجية الأمن السيبراني للجهة.
٢٠	تقييم جهود التطوير للأنظمة والإجراءات الجديدة لضمان تطبيق الضوابط الأمنية المناسبة.
٢١	تحديد استراتيجيات الأمن السيبراني البديلة لتحقيق الغاية الأمنية للجهة.
٢٢	تحديد تبعات التقنيات الجديدة وأعمال الترقية على الأمن السيبراني في جميع أرجاء الجهة.
٢٣	التواصل بفاعلية مع الأطراف الخارجية عند وقوع حادث أمن سيبراني.
٢٤	مراجعة قدرات الأمن السيبراني للتقنيات الجديدة المقترحة قبل تبني الجهة لها، واعتمادها في حال مناسبتها.
٢٥	ضمان الإدارة الملائمة لمعلومات الأمن السيبراني للجهة، وتقييمها ومشاركتها بصفة ملائمة.

#	المسؤوليات
٢٦	مراجعة فاعلية ضوابط الأمن السيبراني للجهة ومواءمتها لأهدافها الاستراتيجية.
٢٧	ضمان التنفيذ الدوري لبرامج التدريب والتوعية بالأمن السيبراني.
٢٨	المشاركة في تقييم مخاطر الأمن السيبراني حسب ما تقتضيه الحاجة.
٢٩	المشاركة في تطوير أو تعديل خطط ومتطلبات برنامج الأمن السيبراني.
٣٠	ضمان تطوير جميع الوثائق الخاصة بأمن الشبكات، وإصدارها وصيانتها.
٣١	ضمان توفير التدريب التوعوي بالأمن السيبراني لجميع الموظفين بالجهة.
٣٢	ضمان إدراج متطلبات الأمن السيبراني في أعمال الشراء حسب الملائم.
٣٣	التأكد من تقديم تقارير مناسبة إلى الإدارة العليا حسب الحاجة.
٣٤	تحديد الحوادث الأمنية المحتملة والإبلاغ عنها حسب الحاجة.
٣٥	التأكد من تخصيص الموارد الملائمة لتحقيق متطلبات الأمن السيبراني بالجهة.
٣٦	إدارة التقييم والصيانة الدورية لسياسات الأمن السيبراني بالجهة والوثائق ذات العلاقة.
٣٧	التأكد من اتخاذ الإجراءات الملائمة لمعالجة الخطر عند وقوع حادثة متعلق بالأمن السيبراني.
٣٨	استخدام الوثائق المتاحة دوليًا ذات العلاقة بالأمن السيبراني لإفادة وتعزيز وثائق الجهة.
٣٩	دعم القضايا الأمنية لدى الإدارة العليا، والتأكد من شمول الأمن السيبراني ضمن الأهداف الاستراتيجية.
٤٠	التأكد من معالجة استراتيجية الأمن السيبراني للجهة بفعالية من خلال سياسات الأمن السيبراني والوثائق ذات الصلة.
٤١	تقييم فاعلية وكفاءة وظيفة المشتريات في ضمان معالجة متطلبات الأمن السيبراني ومخاطر سلسلة الإمداد حسب الحاجة، وتنفيذ التحسينات أينما لزمت.
٤٢	التأكد من تحديد متطلبات الأمن السيبراني لكافة أنظمة تقنية المعلومات.
٤٣	المشاركة في عملية الاستحواذ حسب الضرورة، مع ضمان تبني الممارسات المناسبة لإدارة مخاطر سلسلة الإمداد.
٤٤	التأكد من توفر موارد للأمن السيبراني الملائمة على الدوام.

#	المسؤوليات
٤٥	تطوير سياسات الأمن السيبراني المناسبة والوثائق ذات العلاقة وحفظها لضمان حماية البنية التحتية الحساسة للجهة بشكل ملائم.
٤٦	ضمان المراجعة الدورية للفرضيات ذات العلاقة بالأمن السيبراني.
٤٧	حيازة الموارد الملائمة لتنفيذ وحفظ جوانب الأمن السيبراني لخطة استمرارية أعمال فعالة.
٤٨	إحاطة الإدارة العليا بالتغييرات الهامة في وضع الأمن السيبراني للجهة.
٤٩	التأكد من أن متطلبات الأمن السيبراني لتقنية المعلومات تتوافق مع استراتيجية الأمن السيبراني في الجهة
٥٠	إدارة الجوانب المالية للأمن السيبراني شاملة إعداد الميزانية وتوفير الموارد.
٥١	التأكد من فاعلية إيصال المعلومات التي تخص تهديدات الأمن السيبراني وأساليب معالجتها إلى الأطراف الأخرى المهتمة.
٥٢	المراجعة الدورية لضمان مواءمة سياسات الأمن السيبراني والوثائق ذات العلاقة مع غايات واستراتيجيات الجهة المعلنة.
٥٣	دعم أنشطة الالتزام حسب الحاجة.

مستشار الأمن السيبراني (Cybersecurity Advisor)

#	المسؤوليات
١	التواصل الفعّال مع الإدارة العليا بشأن مخاطر الأمن السيبراني.
٢	التواصل الفعّال مع الإدارة العليا بشأن الجوانب المالية للأمن السيبراني.
٣	العمل مع أصحاب المصلحة لتطوير سياسات الأمن السيبراني والوثائق المصاحبة بما يتوافق مع استراتيجية الأمن السيبراني للجهة.
٤	فهم الحالة الأمنية لمعلومات الجهة والتعبير عنها خلال عمليات التمحيص القانوني والتنظيمي.
٥	دعم الأمن السيبراني وإبراز قيمته لدى أصحاب المصلحة في الجهة.
٦	التواصل بفاعلية مع الأطراف الخارجية عند وقوع حادث أمن سيبراني.

#	المسؤوليات
٧	مراجعة فاعلية ضوابط الأمن السيبراني للجهة ومواءمتها لأهدافها الاستراتيجية.
٨	إدارة التقييم والصيانة الدورية لسياسات الأمن السيبراني بالجهة والوثائق ذات العلاقة.
٩	دعم القضايا الأمنية لدى الإدارة العليا، والتأكد من شمول الأمن السيبراني ضمن الأهداف الاستراتيجية.
١٠	التأكد من معالجة استراتيجية الأمن السيبراني للجهة بفعالية من خلال سياسات الأمن السيبراني والوثائق ذات الصلة.
١١	تزويد الإدارة العليا بموجز عن التطورات والتوجهات في الأمن السيبراني.
١٢	تزويد الإدارة العليا بموجز عن ضوابط الأمن السيبراني اللازمة لحماية الجهة.
١٣	تقييم نواحي الأمن السيبراني عند اختيار وتقييم الموردين.
١٤	إعداد التقارير عن أحداث وفعاليات الأمن السيبراني الدولية لصالح الإدارة العليا.
١٥	إحاطة الإدارة العليا بالتغييرات الهامة في وضع الأمن السيبراني للجهة.
١٦	تطوير وحفظ خطط استراتيجية للأمن السيبراني تتوافق مع خطة الأعمال الاستراتيجية للجهة.
١٧	أداء مهام الاستشاري والمرشد الداخلي في مجال اختصاصه.

أخصائي مخاطر الأمن السيبراني (Cybersecurity Risk Officer)

#	المسؤوليات
١	التواصل الفعّال مع الإدارة العليا بشأن مخاطر الأمن السيبراني.
٢	تطوير أوصاف للمخاطر الأمنية لنظم الحاسب من خلال تقييم التهديدات لتلك النظم وثغراتها.
٣	تطوير استراتيجيات للحد من المخاطر من أجل إدارة المخاطر في ظل سياسات الجهة لمستويات المخاطرة المقبولة.
٤	تطوير إجراءات مضادة خاصة بالأمن السيبراني واستراتيجيات لمعالجة المخاطر.
٥	توصيف مخاطر الأمن السيبراني الأولية أو المتبقية التي تؤثر على تشغيل النظام.

#	المسؤوليات
٦	التأكد من أن القرارات المتخذة بشأن الأمن السيبراني تستند على المبادئ الأساسية لإدارة المخاطر.
٧	تحليل المخاطر كلما خضع أي برنامج أو نظام لتغيير جوهري.
٨	توفير مدخلات لإطار إدارة المخاطر والوثائق ذات الصلة.
٩	ضمان تعريف مخاطر الأمن السيبراني ومعالجتها بالطريقة المناسبة من خلال عملية حوكمة المخاطر للجهة.
١٠	إجراء تقييم لمخاطر الأمن السيبراني.
١١	التعاون مع الآخرين لتنفيذ وحفظ برنامج إدارة مخاطر الأمن السيبراني.
١٢	انتقاء أفراد وإسناد أدوار محددة لهم فيما يتعلق بتنفيذ إطار إدارة المخاطر.
١٣	وضع استراتيجية إدارة المخاطر بالجهة، شاملة تحديد مستوى تحمل المخاطر.
١٤	إجراء تقييم مخاطر أولي لأصول أصحاب المصلحة وتحديث تقييم المخاطر بصفة مستمرة.
١٥	العمل مع المسؤولين بالجهة لضمان أن بيانات أدوات المراقبة المستمرة توفر الوعي بمستويات المخاطر القائمة.
١٦	استخدام أدوات المراقبة المستمرة لتقييم المخاطر باستمرار.
١٧	تطوير منهجيات فعّالة لمراقبة وقياس المخاطر، ومدى الالتزام، وجهود توكيد الالتزام.
١٨	تحديد مخاطر سلسلة الإمداد وتوثيقها لعناصر الأنظمة الحرجة حيثما وجدت.

أخصائي الالتزام في الأمن السيبراني (Cybersecurity Compliance Officer)

#	المسؤوليات
١	تحليل سياسات الدفاع السيبراني للجهة وإعداداتها، وذلك لتقييم مدى التزامها بالتنظيمات والتوجيهات المؤسسية.
٢	تقييم جوانب الأمن السيبراني للعقود لضمان الالتزام بالمتطلبات المالية، والتعاقدية، والقانونية، والتنظيمية.
٣	التأكد من أن أي منتج يتم استخدامه لإدارة مخاطر الأمن السيبراني تم تقييمه بفعالية والتصريح باستخدامه

#	المسؤوليات
٤	التعرف على أنماط عدم الالتزام بسياسات الأمن السيبراني والوثائق ذات العلاقة بهدف تعريف طرق لتحسينها.
٥	المراجعة الدورية لاستراتيجية الأمن السيبراني وسياساته والوثائق ذات العلاقة للمحافظة على الالتزام بالقوانين والأنظمة المعمول بها.
٦	العمل مع أصحاب المصلحة لحل حوادث الأمن السيبراني وقضايا الثغرات في الالتزام.
٧	تطوير منهجيات فعّالة لمراقبة وقياس المخاطر، ومدى الالتزام، وجهود توكيد الالتزام.
٨	تطوير المواصفات لضمان أن جهود معالجة المخاطر والالتزام والضمان تلتزم بمتطلبات الأمن السيبراني.
٩	الحفاظ المتواصل على المعرفة بالسياسات والتنظيمات ووثائق الالتزام المعمول بها في الأمن السيبراني الدفاعي حسب ما يختص منها بأعمال التدقيق للأمن السيبراني الدفاعي.
١٠	مراقبة وتقييم مدى التزام النظام بمتطلبات الأمن السيبراني، ومتطلبات الصمود والاعتمادية.
١١	توفير تقييم تقني صحيح لتطبيقات البرامج أو الأنظمة أو الشبكات، وتوثيق مدى التزامها بمتطلبات الأمن السيبراني المتفق عليها.
١٢	تطوير عمليات الالتزام الأمني وعمليات تدقيق للخدمات المقدمة من أطراف خارجية.
١٣	دعم أنشطة الالتزام حسب الحاجة.
١٤	الحفاظ المتواصل على المعرفة بالقوانين المعمول بها والتنظيمات ومعايير الاعتماد، والمراجعة الدورية لها لضمان التزام الجهة.
١٥	التعاون مع المؤسسات التنظيمية المعنية والكيانات القانونية الأخرى فيما يخص التحقيقات وعمليات مراجعة الالتزام.
١٦	المحافظة على التوعية بقوانين الخصوصية وأنظمتها ومعايير الاعتماد المعمول بها.

أخصائي سياسات الأمن السيبراني (Cybersecurity Policy Officer)

#	المسؤوليات
١	تطوير سياسات الأمن السيبراني والوثائق ذات العلاقة.

#	المسؤوليات
٢	تأسيس قنوات اتصال ملائمة مع أصحاب المصلحة، والحفاظ عليها.
٣	مراجعة السياسات القائمة والمقترحة والوثائق ذات العلاقة مع أصحاب المصلحة.
٤	توفير الخبرة الاستشارية في الأمن السيبراني في مجال السياسات التنظيمية والقطاعية.
٥	ضمان توفير التمويل الكافي لموارد التدريب للأمن السيبراني.
٦	ضمان التزام سياسات وعمليات إدارة كوادر الأمن السيبراني بالمتطلبات القانونية ومتطلبات الجهة.
٧	رفع الوعي بالسياسة والاستراتيجية السيبرانية بين مديري الجهة.
٨	مراجعة وتقييم فاعلية الكوادر السيبرانية لتحديد الفجوات في المهارات واحتياجات التدريب.
٩	تفسير وتطبيق الأنظمة المطبقة والقوانين واللوائح والوثائق التنظيمية لضمان عكسها في سياسات الأمن السيبراني.
١٠	تحليل سياسات الأمن السيبراني للجهة.
١١	العمل مع أصحاب المصلحة لتطوير سياسات الأمن السيبراني والوثائق المصاحبة بما يتوافق مع استراتيجية الأمن السيبراني للجهة.
١٢	موافقة استراتيجية الأمن السيبراني للجهة مع استراتيجيتها للأعمال.
١٣	صياغة ونشر سياسات الأمن السيبراني للجهة.
١٤	مراقبة مدى كفاءة التطبيق لسياسات ومبادئ وممارسات الأمن السيبراني عند تقديم خدمات التخطيط والإدارة.
١٥	السعي إلى توافق آراء أصحاب المصلحة بشأن التغييرات المقترحة في سياسة الأمن السيبراني.
١٦	تقديم إرشادات في حق السياسة لإدارة الأمن السيبراني والعاملين والمستخدمين.
١٧	مراجعة تدقيقات البرامج والمشاريع السيبرانية، أو تنفيذها، أو المشاركة فيها.
١٨	دعم المسؤول الأول لتقنية المعلومات (CIO) في صياغة سياسات الأمن السيبراني.

مقيم ضوابط الأمن السيبراني (Security Controls Assessor)

#	المسؤوليات
١	إجراء مراجعات الأمن السيبراني، وتحديد الفجوات في المعمارية الأمنية، من أجل إصدار خطط لإدارة المخاطر السيبرانية.
٢	إجراء مراجعات الأمن السيبراني، وتحديد الثغرات الأمنية في المعمارية الأمنية لدعم استراتيجيات معالجة المخاطر.
٣	تحليل المخاطر كلما خضع أي برنامج أو نظام لتغيير جوهري.
٤	توفير مدخلات لإطار إدارة المخاطر والوثائق ذات الصلة.
٥	مراجعة وثائق الأمن السيبراني العاكسة لتصميم النظام، وتحديثها وحفظها.
٦	ضمان تعريف مخاطر الأمن السيبراني ومعالجتها بالطريقة المناسبة من خلال عملية حوكمة المخاطر للجهة.
٧	إدارة معالجة الثغرات بفعالية.
٨	ضمان مراعاة متطلبات الجهة للأمن السيبراني في عمليات الدمج والاستحواذ والاستعانة بالموارد الخارجية وغيرها من العمليات التي تشمل طرفا ثالثا.
٩	تقييم فاعلية ضوابط الأمن السيبراني.
١٠	تقييم عملية إدارة الإعدادات.
١١	إدارة حزم الاعتماد والموافقة عليها.
١٢	تخطيط وتنفيذ أعمال المراجعة وتطوير قضايا التصريح الأمني للتثبيت الأولي للنظم والشبكات.
١٣	مراجعة سجلات المخاطر والوثائق المشابهة للتأكد من أن مستوى المخاطر لكل تطبيق ونظام وشبكة يقع ضمن الحدود المقبولة.
١٤	إجراء أعمال التدقيق للحالة الأمنية للبرامج والشبكة والنظام حسب ما ورد في سياسات الأمن السيبراني، وتقديم توصيات بالأنشطة المطلوبة لعلاج الثغرات المكتشفة.
١٥	تطوير عمليات الالتزام الأمني وعمليات تدقيق للخدمات المقدمة من أطراف خارجية.

#	المسؤوليات
١٦	المراجعة الدورية لضمان مواءمة سياسات الأمن السيبراني والوثائق ذات العلاقة مع غايات واستراتيجيات الجهة المعلنة.
١٧	تحديد وتوثيق أثر تنفيذ نظام جديد أو واجهات اتصال جديدة بين النُظم على الوضع الأمني للبيئة الحالية.
١٨	ضمان توثيق التصميم والتطوير لأنشطة الأمن السيبراني على نحو ملائم.
١٩	دعم أنشطة الالتزام حسب الحاجة.
٢٠	ضمان أن إعدادات التطبيقات والشبكات والنُظم تلتزم بسياسات الجهة للأمن السيبراني.

أخصائي قانون الأمن السيبراني (Cybersecurity Legal Specialist)

#	المسؤوليات
١	تقييم جوانب الأمن السيبراني للعقود لضمان الالتزام بالمتطلبات المالية، والتعاقدية، والقانونية، والتنظيمية.
٢	إدارة النظم على نظم وبرامج مخصصة للأمن السيبراني.
٣	فهم الحالة الأمنية لمعلومات الجهة والتعبير عنها خلال عمليات التمحيص القانوني والتنظيمي.
٤	تقييم فاعلية السياسات أو المعايير أو الإجراءات في تحقيق استراتيجية الجهة.
٥	تفسير وتطبيق القوانين والأنظمة والسياسات أو الإجراءات حسب الحاجة.
٦	حل التعارضات بين السياسات أو المعايير أو الإجراءات عند خلافها مع القوانين والتنظيمات المعمول بها.

#	المسؤوليات
٧	اكتساب المعرفة العملية بالمشاكل الدستورية التي تنشأ في القوانين والأنظمة والسياسات والاتفاقيات والمعايير والإجراءات، والحفاظ عليها على الدوام.
٨	توفير الخبرات بالأمن السيبراني عند تأطير المرافعات طلبا لتحديد أيّ انتهاكات مزعومة للقوانين، أو الأنظمة أو السياسات أو الإرشادات.
٩	تطوير الإرشادات الخاصة بتنفيذ ضوابط الأمن السيبراني ذات العلاقة.
١٠	توفير إرشادات في الأمن السيبراني للمشرفين وموظفي متابعة الالتزام فيما يخص الالتزام بسياسات الأمن السيبراني والمتطلبات القانونية والتنظيمية ذات الصلة.
١١	تقييم أثر التغييرات في القوانين والأنظمة على سياسات الأمن السيبراني بالجهة والوثائق ذات العلاقة.
١٢	توفير إرشادات من منظور الأمن السيبراني بشأن القوانين والأنظمة والسياسات والمعايير، أو الإجراءات لصالح الإدارة، أو العاملين، أو العملاء.
١٣	المساعدة في تنفيذ القوانين أو الأنظمة أو الأوامر التنفيذية وما شابهها – سواء كانت جديدة أم محدثة - حسب علاقتها بسياسات الأمن السيبراني والوثائق الأخرى.
١٤	توفير الإرشاد من منظور الأمن السيبراني فيما يخص إعداد الوثائق القانونية والوثائق الأخرى ذات الصلة.
١٥	المحافظة على التوعية بقوانين الخصوصية وأنظمتها ومعايير الاعتماد المعمول بها.

محلل دفاع الأمن السيبراني (Cybersecurity Defense Analyst)

#	المسؤوليات
١	ربط بيانات الحوادث لتحديد الثغرات
٢	استخدام منتجات الأمن السيبراني أو تقنيات التحكم الأمني للحد من المخاطر المكتشفة إلى مستويات مقبولة.
٣	توثيق وتصعيد الحوادث السيبرانية التي من شأنها أن تؤدي إلى أثر فوري أو مستمر.
٤	تحليل توجهات الدفاع السيبراني، وتقديم تقارير بشأنها.
٥	ربط المعلومات من مصادر متعددة للإلمام بالحالة وتحديد فاعلية الهجمة المرصودة.

#	المسؤوليات
٦	إجراء مراجعات الأمن السيبراني، وتحديد الثغرات الأمنية في المعمارية الأمنية لدعم استراتيجيات معالجة المخاطر.
٧	تحليل نتائج التمارين وبيئة النظام للتخطيط وللتوصية بتعديلات وتسويات.
٨	تحليل تنبيهات الشبكة التي يتم الحصول عليها من مصادر مختلفة لتحديد الأسباب المحتملة لأي أحداث يتم اكتشافها.
٩	الكشف عن الهجمات والأنشطة المشبوهة وحالات إساءة الاستخدام، والتعرف عليها والتنبيه بشأنها في الوقت المناسب، وتمييزها عن الأنشطة الاعتيادية.
١٠	تسخير أدوات الدفاع السيبراني للمراقبة المستمرة لأنشطة النظم وتحليلها بهدف تعريف الأنشطة الضارة.
١١	تحليل الأنشطة الخبيثة لتحديد الثغرات المستغلة، وأساليب الاستغلال، والتأثيرات على النظم والمعلومات.
١٢	تحديد الخطط والأساليب والإجراءات (TTP) لمجموعات التسلل.
١٣	فحص المخططات الشبكية لفهم تدفقات البيانات عبر الشبكة.
١٤	التوصية بتصحيحات لثغرات البيئة.
١٥	استخدام البيانات الوصفية للتعرف على حالات الاشتباه في حركة مرور البيانات عبر الشبكة وتحليلها.
١٦	تحديد المؤشرات والتحذيرات من خلال البحث والتحليل والربط عبر مجموعات بيانات متعددة.
١٧	استخدام أدوات تحليل الحزم للتحقق من تنبيهات نظام كشف التسلل.
١٨	عزل البرمجيات الضارة وإزالتها.
١٩	استخدام حركة مرور البيانات عبر الشبكة لتحديد تطبيقات أحد أجهزة الشبكة ونظم التشغيل الخاصة به.
٢٠	استخدام حركة المرور عبر الشبكات لإعادة تمثيل النشاط الخبيث.
٢١	تحديد عمليات محاولة التعرف على التصميم الشبكي وأنشطة التعرف على أنظمة التشغيل.
٢٢	المساعدة في حصر خواص التعرف (التواقيع) لتفعيل استخدامها في أدوات الأمن السيبراني للشبكة وذلك للاستجابة للتهديدات الجديدة والتهديدات التي تمت ملاحظتها سابقًا.

#	المسؤوليات
٢٣	الإبلاغ عن الحوادث السيبرانية المشتبه بها وفقًا لخطة الجهة للاستجابة للحوادث السيبرانية.
٢٤	تحليل التوجهات في الحالة الأمنية للجهة، والإبلاغ عنها.
٢٥	تقييم مدى كفاية ضوابط التحكم بالوصول بناء على سياسات الجهة.
٢٦	مراقبة مصادر البيانات الخارجية للمحافظة على فهم محدث لحالة تهديدات الأمن السيبراني وتحديد القضايا الأمنية التي قد تؤثر على الجهة.
٢٧	تقييم ومراقبة جوانب الأمن السيبراني لممارسات الجهة بتطبيق النُظم واختبارها.
٢٨	تقديم توصيات الأمن السيبراني للقيادة استنادًا إلى التهديدات والثغرات الجسيمة.
٢٩	العمل مع أصحاب المصلحة لحل حوادث الأمن السيبراني وقضايا الثغرات في الالتزام.
٣٠	تطوير أدوات الدفاع السيبراني.
٣١	وصف وتحليل حركة المرور على الشبكة، لتحديد الأنشطة الشاذة والتهديدات المحتملة لموارد الشبكات.
٣٢	التنسيق مع بقية طاقم عمل الدفاع السيبراني للتحقق من مصداقية التنبيهات الشبكية.
٣٣	تقديم تقارير مُجملة يومية لأحداث الشبكات والأنشطة الأخرى ذات الصلة بالأمن السيبراني بما يتلاءم مع سياسات ومتطلبات الجهة.

أخصائي البنية التحتية للأمن السيبراني (Cybersecurity Infrastructure Specialist)

#	المسؤوليات
١	تطبيق السياسات الأمنية لتحقيق الأهداف الأمنية للنظام.
٢	إدارة النظم على نظم وبرامج مخصصة للأمن السيبراني.
٣	تحديد حماية البنية التحتية الحاسمة للدفاع السيبراني ومواردها، وترتيب أولوياتها وتنسيقها.
٤	تطبيق وظائف الأمن السيبراني (مثل التشفير والتحكم في الوصول وإدارة الهوية) لتقليل فرص الاستغلال.
٥	الإدارة والإشراف على أعمال تحديث القواعد والتواقيع لتطبيقات الدفاع السيبراني.

#	المسؤوليات
٦	إعداد وتهيئة برامج وأجهزة الدفاع السيبراني المخصصة، وتثبيتها وتحديثها واختبارها.
٧	المساعدة في تقييم أثر بناء وتشغيل بنية تحتية مخصصة للدفاع السيبراني.
٨	إدارة منصات الاختبار، واختبار وتقييم التطبيقات وأجهزة البنية التحتية والقواعد والتوقيعات، وضوابط التحكم بالوصول وإعدادات المنصات التي يديرها مزودو الخدمات.
٩	إنشاء قوائم التحكم بالوصول إلى الشبكات المخزنة بداخل نُظم الدفاع السيبراني المخصصة، وتعديلها وإدارتها.
١٠	تحديد التعارضات المحتملة جراء تنفيذ أي من أدوات الدفاع السيبراني، والإبلاغ عنها.
١١	تنفيذ متطلبات إطار إدارة المخاطر والتقييم الأمني والتصريح لنُظم الدفاع السيبراني المخصصة داخل الجهة، وتوثيق سجلاتها وحفظها.
١٢	انتقاء ضوابط الأمن السيبراني للنظام وتوثيق الوصف الوظيفي لتنفيذ الضوابط في الخطة الأمنية.
١٣	تنفيذ ضوابط الأمن السيبراني الواردة في الخطة الأمنية أو وثائق النُظم الأخرى.
١٤	تطوير العمليات والإجراءات الخاصة بالتحديث وعمل تحديث الإصلاح اليدوي لبرمجيات النُظم بحسب متطلبات الجدول الزمني الحالي أو المتوقع لتطبيق حزم تحديثات الإصلاح على البيئة التشغيلية للنظام.

أخصائي الأمن السيبراني (Cybersecurity Specialist)

#	المسؤوليات
١	تطبيق السياسات الأمنية لتحقيق الأهداف الأمنية للنظام.
٢	ربط بيانات الحوادث لتحديد الثغرات.
٣	تحليل السجلات من مصادر متعددة لتحديد التهديدات المحتملة لأمن الشبكة.
٤	تحليل توجهات الدفاع السيبراني، وتقديم تقارير بشأنها.

#	المسؤوليات
٥	تقييم ومراقبة جوانب الأمن السيبراني لممارسات الجهة بتطبيق النُظم واختبارها.
٦	أداء تقييمات تقنية وغير تقنية للمخاطر والثغرات للبيئات التقنية للجهة.
٧	تقديم توصيات لتمكين المعالجة الفعّالة للثغرات.
٨	تطوير أدوات الدفاع السيبراني.
٩	وصف وتحليل حركة المرور على الشبكة، لتحديد الأنشطة الشاذة والتهديدات المحتملة لموارد الشبكات.
١٠	التنسيق مع بقية طاقم عمل الدفاع السيبراني للتحقق من مصداقية التنبيهات الشبكية.
١١	تقديم تقارير مُجملة يومية لأحداث الشبكات والأنشطة الأخرى ذات الصلة بالأمن السيبراني بما يتلاءم مع سياسات ومتطلبات الجهة.

أخصائي تقييم الثغرات (Vulnerability Assessment Specialist)

#	المسؤوليات
١	تحليل سياسات الدفاع السيبراني للجهة وإعداداتها، وذلك لتقييم مدى التزامها بالتنظيمات والتوجيهات المؤسسية.
٢	ربط بيانات الحوادث لتحديد الثغرات.
٣	الحفاظ على مجموعة أدوات تدقيق الدفاع السيبراني القابلة للتفعيل، بناء على أفضل الممارسات في القطاع، وذلك لدعم عمليات تدقيق الدفاع السيبراني.
٤	إعداد تقارير التدقيق والتقييم التي تحدد النتائج التقنية والإجرائية، وتشمل توصيات بالاستراتيجيات والحلول العلاجية.
٥	أداء تقييمات تقنية وغير تقنية للمخاطر والثغرات للبيئات التقنية للجهة.
٦	استخدام أدوات المراقبة المستمرة لتقييم المخاطر باستمرار.
٧	الحفاظ المتواصل على المعرفة بالسياسات والتنظيمات ووثائق الالتزام المعمول بها في الأمن السيبراني الدفاعي حسب ما يختص منها بأعمال التدقيق للأمن السيبراني الدفاعي.

#	المسؤوليات
٨	إجراء أو دعم اختبارات الاختراق المصرحة للبنية التحتية والأصول.
٩	إجراء المراجعات المطلوبة شاملة مراجعات التدابير الدفاعية حسب سياسات الجهة.
١٠	تقديم التوصيات بخصوص الضوابط الأمنية ذات الكفاءة المالية لمعالجة المخاطر المكتشفة عن طريق الاختبار والمراجعة.
١١	مسح الثغرات على الأنظمة والأصول.
١٢	استخدام الاختبارات الأمنية وأدوات مسح الشفرات لمراجعة الشفرات.

أخصائي اختبار الاختراقات (Penetration Tester/Red Team Specialist)

#	المسؤوليات
١	إجراء أو دعم اختبارات الاختراق المصرحة للبنية التحتية والأصول.
٢	جمع المعلومات عن معمارية واستخدامات الشبكات من خلال التحليل التقني والبحث في المصادر المفتوحة وتوثيق النتائج.
٣	محاكاة أساليب الهندسة الاجتماعية الضارة التي يستخدمها المهاجم في محاولته لخرق النظام للكشف عن الثغرات الأمنية ونقاط الضعف.
٤	تحديد المنهجيات التي قد يستخدمها المهاجمون لاستغلال نقاط الضعف في النُظم والشبكات.
٥	أخذ الأعمال في الاعتبار وتضمينها في توصيات واستراتيجيات الأمن السيبراني.
٦	مسح الثغرات على الأنظمة والأصول.
٧	إعداد تقارير نتائج اختبارات الاختراق والتقييم لنقاط الضعف شاملا مستوى الخطر، واقتراحات المعالجة، وكافة التفاصيل التقنية اللازمة لإعادة توليد نتائج الاختبار.
٨	مناقشة النتائج الأمنية مع الإدارة المعنية بالأمن السيبراني والإدارة العليا وفرق تقنية المعلومات.
٩	تصميم وتطوير عمليات اختبارات الاختراق.
١٠	إجراء اختبار عن بُعد للشبكة للكشف عن نقاط الضعف الأمنية.

#	المسؤوليات
١١	تخطيط وإنشاء منهجيات وبرمجيات واختبارات الاختراق.
١٢	تصميم نماذج محاكاة للهجمات لتوضح الأثر على أعمال الجهة والمستخدمين.
١٣	عرض نتائج الاختبارات والمخاطر والاستنتاجات على المتلقين التقنيين وغير التقنيين.
١٤	توضيح التبعات على الأعمال بسبب نقاط الضعف المكتشفة من خلال الاختبارات لإبراز أهمية معالجتها.
١٥	إجراء التقييمات الأمنية المادية للخوادم والنُظم وأجهزة الشبكات.
١٦	فحص الثغرات في التطبيقات على الشبكة العنكبوتية الإنترنت وتطبيقات العميل والتطبيقات النمطية.
١٧	تحديد مصطلحات اللغات الأجنبية بداخل برامج الحاسب (مثل الملاحظات وأسماء المتغيرات).

أخصائي استجابة للحوادث السيبرانية (Cybersecurity Incident Responder)

#	المسؤوليات
١	ربط بيانات الحوادث لتحديد الثغرات.
٢	تحليل السجلات من مصادر متعددة لتحديد التهديدات المحتملة لأمن الشبكة.
٣	تحليل أولويات الحوادث لتحديد الثغرة ونطاقها وأولويتها وتأثيرها المحتمل، ومن ثم تقديم توصيات من شأنها توفير المعالجة السريعة.
٤	تحليل توجهات الدفاع السيبراني، وتقديم تقارير بشأنها.
٥	إجراء جمع أولي للصور الجنائية بموجب معايير البحث الجنائي ذات العلاقة، وفحصها لتحديد أنسب إجراءات المعالجة
٦	أداء مهام الاستجابة للأحداث دعما لفرق الاستجابة للأحداث، شاملا جمع الأدلة الجنائية، وربط حالات التسلل، والتتبع، وتحليل التهديدات ومعالجة الأنظمة.
٧	تحليل تنبيهات الشبكة التي يتم الحصول عليها من مصادر مختلفة لتحديد الأسباب المحتملة لأي أحداث يتم اكتشافها.

#	المسؤوليات
٨	تتبع الحوادث السيبرانية وتوثيقها منذ اكتشافها إلى حلها بشكل نهائي.
٩	كتابة ونشر أساليب وإرشادات تعزيز الأمن السيبراني وتقارير الأحداث السيبرانية، ومشاركتها مع الجهات ذات العلاقة.
١٠	تطبيق مبادئ وممارسات الدفاع الأمني متعدد المستويات بما يتماشى مع سياسات الجهة.
١١	جمع آثار التسلل، واستخدام البيانات المكتشفة للحد من حوادث الأمن السيبراني المحتملة داخل الجهة.
١٢	تحرير ونشر المراجعات للتعلم ولنشر الدروس المستفادة من أحداث الأمن السيبراني.
١٣	مراقبة مصادر البيانات الخارجية للمحافظة على فهم محدث لحالة تهديدات الأمن السيبراني وتحديد القضايا الأمنية التي قد تؤثر على الجهة.
١٤	تنسيق وظائف الاستجابة للحوادث.
١٥	تقديم الدعم التقني من الخبراء لحل حوادث الدفاع السيبراني.
١٦	أداء دور الخبير التقني لدعم السلطات القانونية التنفيذية وشرح تفاصيل حادث الأمن السيبراني والتحليل الجنائي، حسب المطلوب.
١٧	التنسيق مع محللي معلومات التهديدات السيبرانية بهدف ربط بيانات تقييم التهديدات.
١٨	الإبلاغ عن الحوادث السيبرانية لإفادة الدفاع السيبراني.
١٩	تحديد وانتقاء موارد المعلومات الأكثر فاعلية للمساعدة في التحقيق في حادث الأمن السيبراني.

أخصائي التحليل الجنائي الرقمي (Digital Forensics Specialist)

#	المسؤوليات
١	فك تشفير البيانات المضبوطة باستخدام وسائل تقنية.

#	المسؤوليات
٢	تحليل الخصائص المميزة للملفات.
٣	إجراء تحليل جنائي رقمي فعلي.
٤	تحليل الخط الزمني للأحداث.
٥	أداء مهام الاستجابة للأحداث دعما لفرق الاستجابة للأحداث، شاملا جمع الأدلة الجنائية، وربط حالات التسلل، والتتبع، وتحليل التهديدات ومعالجة الأنظمة.
٦	استخدام أدوات مراقبة الشبكات لرصد وتحليل حركة البيانات الشبكية ذات العلاقة بالعمليات الضارة
٧	تحليل ملفات السجلات والأدلة والمعلومات الأخرى لتحديد أفضل المنهجيات لمعرفة هوية المتسلل للشبكة.
٨	تأكيد ما هو معلوم عن عملية التسلل والسعي لاكتشاف معلومات جديدة.
٩	إنشاء نسخة مطابقة وسليمة من جانب الأدلة الشرعية بهدف استخدامها في عمليات استعادة البيانات وتحليلها، تمشيا مع السياسات المعنية سواء المؤسسية منها أو الوطنية حسب الساري.
١٠	تقديم ملخص تقني للنتائج وفقًا لإجراءات الإبلاغ القائمة.
١١	ضمان تتبع تسلسل العُهَد لجميع الوسائط الرقمية المستحوذ عليها وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.
١٢	تحديد الأدلة الرقمية للفحص والتحليل.
١٣	إجراء تحليل ديناميكي لتحميل "صورة" (نسخة طبق الأصل من البيانات) لمحرك الأقراص - سواء مع أو بدون وجود محرك الأقراص الأصلي- لرؤية التسلل كما قد يراه المستخدم في بيئة أصلية.
١٤	إجراء مقارنة الاختزال (Hash comparison) على قواعد البيانات حسب متطلبات سياسات الجهة.
١٥	إجراء تحليل للوسائط غير القابلة للتغيير.
١٦	إجراء تحليل للبرمجيات الضارة على المستوى الأول والثاني والثالث.
١٧	ضمان سلامة البيانات عند إعداد الوسائط الرقمية للنسخ.
١٨	تقديم مساعدة تقنية خلال عمليات جمع وحفظ ومعالجة أو تحليل الأدلة الرقمية.

#	المسؤوليات
١٩	التعرف على الوحدات الجنائية الأولية والإبلاغ عنها بما يتماشى مع سياسات الإبلاغ.
٢٠	استخلاص البيانات من الأجهزة.
٢١	استخدام معدات وأساليب مخصصة للقيام بمهام التحقيق الجنائي الرقمي بما يتماشى مع السياسات.
٢٢	إجراء تحليل سريع على مستوى الشفرات الثنائية.
٢٣	أداء دور الخبير التقني لدعم السلطات القانونية التنفيذية وشرح تفاصيل حادث الأمن السيبراني والتحليل الجنائي، حسب المطلوب.
٢٤	فحص الفيروسات على الوسائط الرقمية.
٢٥	إجراء تحليل جنائي لأنظمة إدارة الملفات.
٢٦	إجراء تحليل ثابت لتحميل "صورة" (نسخة طبق الأصل من البيانات) لقرص مع وجود القرص الأصلي أو بدونه.
٢٧	إجراء تحليل ثابت للبرمجيات الضارة.
٢٨	استخدام مجموعة الأدوات الجنائية القابلة للتطبيق الميداني لدعم العمليات.
٢٩	التنسيق مع محللي معلومات التهديدات السيبرانية بهدف ربط بيانات تقييم التهديدات.
٣٠	معالجة نسخة البيانات بأدوات تناسب غايات التحقيق.
٣١	إجراء تحليل لسجل Windows المركزي.
٣٢	مراقبة الملفات والسجل المركزي على نظام التشغيل الحي، بعد تحديد التسلل.
٣٣	إدخال معلومات الوسائط الرقمية التي تمت حيازتها إلى قاعدة بيانات التتبع.
٣٤	الإبلاغ عن الحوادث السيبرانية لإفادة الدفاع السيبراني.
٣٥	بناء أدوات للحوادث السيبرانية القابلة للتطبيق الميداني.
٣٦	استخدام نتائج تحليل آثار التسلل لإفادة التوصيات بشأن معالجة حوادث الدفاع السيبراني المحتملة.
٣٧	مراجعة النسخ طبق الأصل من البيانات الجنائية والبيانات العُرضة للتغيير وغيرها من مصادر البيانات لاستعادة المعلومات التي يُحتمل أن تكون ذات صلة.

#	المسؤوليات
٣٨	تحرير ونشر التوصيات والتقارير عن مكتشفات الحوادث لصالح المجموعات المعنية.
٣٩	فحص البيانات المستردة بحثًا عن معلومات ذات الصلة بالمشكلة محل النظر.
٤٠	تحديد التسلل من خلال إجراء تحليل ديناميكي.
٤١	القيام بتحليل البرمجيات الضارة ذات المستوى الأول والثاني.

أخصائي تحقيقات الجرائم السيبرانية (Cyber Crime Investigator)

#	المسؤوليات
١	بناء علاقات بين فريق الاستجابة للحوادث والمجموعات الداخلية والخارجية الأخرى.
٢	تحديد البيانات التي ستضيف قيمة لعمليات التحقيق.
٣	عقد مقابلات مع الضحايا المحتملين للجرائم السيبرانية ومع الشهود.
٤	تطوير خطة للتحقيق في الجرائم السيبرانية المزعومة أو المخالفة أو النشاط المشتبه به.
٥	دمج نتائج التحليل للشبكات وللبنية التحتية وللأدلة الرقمية مع النتائج من التحقيقات والعمليات الجنائية الأخرى.
٦	تحديد ما إذا كان الحادث الأمني يُعد مخالفًا للقانون وبالتالي يتطلب اتخاذ إجراء قانوني محدد.
٧	تحديد الأدلة الرقمية للفحص والتحليل.
٨	تحديد الأدلة التي يمكن أن تثبت وقوع جريمة سيبرانية.
٩	تحديد الأدلة النصية أو المادية المرتبطة بحوادث التسلل السيبرانية والتحقيقات والعمليات، وجمعها والاستحواذ عليها.
١٠	إدارة مسرح الجريمة.
١١	تأمين الأجهزة الإلكترونية ومصادر المعلومات المطلوبة للتحليل.
١٢	استخدام معدات وأساليب مخصصة للقيام بمهام التحقيق الجنائي الرقمي بما يتماشى مع السياسات.

#	المسؤوليات
١٣	تقييم الأفعال والتصرفات ذات العلاقة بعمليات التحري مع الضحايا والشهود أو المشتبه بهم، ورفع تقارير بذلك.
١٤	تحديد نطاق تغطية التهديدات، والمخاطر الناجمة، وتقديم توصية بالأفعال أو التدابير المضادة لمعالجتها.
١٥	تقديم الدعم بخصوص التحقيقات الجنائية للسلطات القانونية خلال مجريات العملية القضائية.
١٦	الإبلاغ عن الحوادث السيبرانية لإفادة الدفاع السيبراني.
١٧	تحليل المواد المتعلقة بحوادث الأمن السيبراني للحصول على أدلة على وجود طرف أجنبي عدائي أو نشاط إجرامي.
١٨	جمع وحفظ الأدلة التي يمكن استخدامها في مقاضاة مقترفي الجرائم السيبرانية.
١٩	تحديد وتطوير دلائل ومصادر معلومات للمساعدة في تحديد الأطراف المسؤولة عن الجرائم السيبرانية أو مقاضاتهم.
٢٠	توثيق الحالة الأصلية للأدلة الرقمية والأدلة ذات الصلة بما يتوافق مع السياسات الوطنية وسياسات الجهة.
٢١	تحليل نُظم تقنية المعلومات والوسائط الرقمية لحل الجرائم السيبرانية والتحقيق فيها، وللمقاضاة.
٢٢	توثيق مجريات التحقيق وفقًا للمعايير والمتطلبات القانونية.
٢٣	تحديد وانتقاء موارد المعلومات الأكثر فاعلية للمساعدة في التحقيق في حادث الأمن السيبراني.
٢٤	فحص البيانات المستردة بحثًا عن معلومات ذات الصلة بالمشكلة محل النظر.
٢٥	عقد المقابلات مع المشتبه بارتكابهم جرائم سيبرانية.

أخصائي الهندسة العكسية للبرمجيات الضارة (Malware Reverse Engineering Specialist)

#	المسؤوليات
١	تحديد وتطوير أدوات الهندسة العكسية لتعزيز القدرات والكشف عن الثغرات.

#	المسؤوليات
٢	مراجعة وتحليل تهديدات الأمن السيبراني لتزويد أصحاب المصلحة بالمعلومات المطلوبة للاستجابة لهذه التهديدات.
٣	إجراء تحليل للبرمجيات الضارة على الرُتبة الأولى والثانية والثالثة.
٤	مراجعة المعلومات المجموعة لتحديد مدى مصداقيتها وعلاقتها بالتحقيق بما يتوافق مع سياسات الجهة
٥	تنقيح التقارير لحماية بيانات أو منهجيات الممتلكات الخاصة، أو التجارية، أو الشخصية، أو غيرها من البيانات أو المنهجيات السرية أو الحساسة.
٦	توثيق الدروس المستفادة من مخرجات الأحداث والتمارين.
٧	تحديد أيّ نشاط خبيث محتمَل من خلال تفريغ الذاكرة، أو السجلات، أو الحِزم الملتقطة.
٨	إجراء التحليل العقدي الشبكة.
٩	تحديد أساليب التهديد ومنهجياته.
١٠	مراقبة أنشطة التهديد التي تم التحقق منها والإبلاغ عنها.
١١	القيام بتحليل البرمجيات الضارة ذات المستوى الأول والثاني.
١٢	المحافظة على تصور مشترك للمعلومات الاستباقية.
١٣	القيام بأبحاث وعمليات تحليل متعمقة.
١٤	تطوير متطلبات المعلومات اللازمة للاستجابة لطلبات المعلومات ذات الأولوية.
١٥	إنشاء طلبات للمعلومات.
١٦	إصدار معلومات استباقية مدمجة وفي الوقت المناسب من كافة مصادر العمليات السيبرانية ومن دلائل وتحذيرات منتجات المعلومات الاستباقية (مثل تقييمات التهديدات، والإيجازات، ودراسات المعلومات الاستباقية، ودراسات الدول).
١٧	توفير دعم المعلومات الاستباقية الآني لأصحاب المصلحة الداخليين والخارجيين المهمين، حسب الملائم.
١٨	توفير التقييم والمرئيات اللازمة لتحسين إنتاج المعلومات الاستباقية و تقاريرها عمليات ومتطلبات جمعها.

#	المسؤوليات
١٩	توفير تحذيرات آنية بالمقاصد، أو الأنشطة الوشيكة أو العدائية، أو الأنشطة التي قد تؤثر على غايات الجهة أو مواردها أو قدراتها.
٢٠	تحديد أساليب ومنهجيات التهديد السيبراني.
٢١	تحديد مصطلحات اللغات الأجنبية بداخل برامج الحاسب (مثل الملاحظات وأسماء المتغيرات).

محلل معلومات التهديدات السيبرانية (Threat Intelligence Analyst)

#	المسؤوليات
١	تتبع حالة طلبات المعلومات، بما يتوافق مع سياسات الجهة.
٢	الإجابة عن طلبات المعلومات بما يتوافق مع سياسات الجهة.
٣	استخدام المعرفة بممثلي التهديد وبالأنشطة لبناء فهم مشترك عن حالة المخاطر الحالية للجهة.
٤	استخدام المعرفة بممثلي التهديد وبالأنشطة لإفادة الجهة في الاستجابة لحادث سيبراني.
٥	تنسيق مصادر المعلومات الاستباقية لتهديدات الأمن السيبراني ونقاط التغذية، والتحقق من مصداقيتها وإدارتها.
٦	تحديد الثغرات في المعلومات الاستباقية للتهديدات وتقييم آثارها على الجهة.
٧	إعداد وتقديم ملخصات عن تهديدات معينة للجهة.
٨	التعاون ومشاركة المعلومات مع محللي معلومات التهديدات الذين يعملون في المجالات ذات الصلة.
٩	إجراء التحليل العقدي الشبكة.
١٠	تقييم عمليات صنع القرار بشأن التهديدات.
١١	تحديد التهديدات الأساسية للثغرات المعروفة بالجهة.
١٢	تحديد أساليب التهديد ومنهجياته.
١٣	المراقبة والإبلاغ عن التغيرات في ميول التهديدات وأنشطتها، وأساليبها، وقدراتها، وغاياتها.
١٤	مراقبة أنشطة التهديد التي تمت مصادقتها والإبلاغ عنها.

#	المسؤوليات
١٥	مراقبة المواقع مفتوحة المصدر للمحتوى العدائي الموجه ضد مصالح الجهة أو شركائها.
١٦	مراقبة أنشطة الجهات التي تمثل مصدر للتهديدات والإبلاغ عنها، لتحقيق متطلبات الجهة المتعلقة بالمعلومات الاستباقية للتهديدات والبلاغات.
١٧	تسخير الخبرة حيال ممثلي التهديد لدعم أنشطة التخطيط والتطوير لاستراتيجية وموارد الأمن السيبراني للجهة.
١٨	توفير المعلومات والتقييمات عن ممثلي التهديد لدعم أصحاب المصلحة في تخطيط وتنفيذ أنشطة الأمن السيبراني
١٩	تقديم التحليل والدعم الحي في مجال المعلومات الاستباقية للتهديدات خلال تمارين وحوادث الأمن السيبراني.
٢٠	مراقبة مصادر التغذية للمعلومات الاستباقية للتهديدات والإبلاغ عن الأحداث الشبكية الكبيرة وحالات التسلل.
٢١	المحافظة على تصور مشترك للمعلومات الاستباقية.
٢٢	القيام بأبحاث وعمليات تحليل متعمقة.
٢٣	تطوير متطلبات المعلومات اللازمة للاستجابة لطلبات المعلومات ذات الأولوية.
٢٤	إنشاء طلبات للمعلومات.
٢٥	إصدار معلومات استباقية مدمجة وفي الوقت المناسب من كافة مصادر العمليات السيبرانية ومن دلائل وتحذيرات منتجات المعلومات الاستباقية (مثل تقييمات التهديدات، والإيجازات، ودراسات المعلومات الاستباقية، ودراسات الدول).
٢٦	توفير دعم المعلومات الاستباقية الآني لأصحاب المصلحة الداخليين والخارجيين المهمين، حسب الملائم.
٢٧	توفير التقييم والتغذية الراجعة اللازمة لتحسين إنتاج المعلومات الاستباقية وتقاريرها عمليات ومتطلبات جمعها
٢٨	توفير إخطارات آنية بالمقاصد، أو الأنشطة الوشيكة، أو العدائية، أو الأنشطة التي قد تؤثر على غايات الجهة أو مواردها أو قدراتها.
٢٩	العمل الوثيق مع المخططين ومحللي معلومات التهديدات ومديري التجميع؛ لضمان دقة وحداثة متطلبات المعلومات الاستباقية وخطط تجميعها.

#	المسؤوليات
٣٠	تحديد أساليب ومنهجيات التهديد السيبراني.

أخصائي اكتشاف التهديدات السيبرانية (Threat Hunter)

#	المسؤوليات
١	ربط بيانات الحوادث لتحديد الثغرات.
٢	تأسيس قنوات اتصال ملائمة مع أصحاب المصلحة، والحفاظ عليها.
٣	إنشاء علاقات بين فريق الاستجابة للحوادث والمجموعات الداخلية والخارجية الأخرى.
٤	تحديد البيانات التي ستضيف قيمة لعمليات التحقيق.
٥	تحليل السجلات من مصادر متعددة لتحديد التهديدات المحتملة لأمن الشبكة.
٦	تحليل أولويات الحوادث لتحديد الثغرة ونطاقها وأولويتها وتأثيرها المحتمل، ومن ثم تقديم توصيات من شأنها توفير العلاج السريع.
٧	تحليل توجهات الدفاع السيبراني، وتقديم تقارير بشأنها.
٨	تحليل الملفات لتحديد سماتها المميزة.
٩	إجراء تحليل جنائي رقمي حي.
١٠	تحليل الخط الزمني للأحداث.
١١	أداء مهام الاستجابة للأحداث دعما لفرق الاستجابة للأحداث، شاملا جمع الأدلة الجنائية، وربط حالات التسلل، والتتبع، وتحليل التهديدات ومعالجة الأنظمة.
١٢	أداء البرمجة الآمنة وتحديد مواطن الخلل المحتملة في الشفرات البرمجية لمعالجة الثغرات.
١٣	تسخير أدوات مراقبة الشبكات لرصد وتحليل حركة البيانات الشبكية ذات العلاقة بالعمليات الضارة.
١٤	الكشف عن الهجمات والأنشطة المشبوهة وحالات إساءة الاستخدام، والتعرف عليها والتنبيه بشأنها في الوقت المناسب، وتمييزها عن الأنشطة الاعتيادية.

#	المسؤوليات
١٥	تسخير أدوات الدفاع السيبراني للمراقبة المستمرة لأنشطة النظم وتحليلها بهدف تعريف الأنشطة الضارة.
١٦	تحليل الأنشطة الخبيثة لتحديد الثغرات المستغلة، وأساليب الاستغلال، والتأثيرات على النظم والمعلومات.
١٧	تحديد حماية البنية التحتية الحاسمة للدفاع السيبراني ومواردها، وترتيب أولوياتها وتنسيقها.
١٨	ضمان الحفاظ على سجل تدقيق أدلة التدابير الأمنية.
١٩	استخدام أدوات تحليل الحزم للتحقق من تنبيهات نظام كشف التسلل.
٢٠	جمع المقاييس وبيانات التوجهات.
٢١	تحديد وتطوير أدوات الهندسة العكسية لتعزيز القدرات والكشف عن الثغرات.
٢٢	مراجعة تدقيقات البرامج والمشاريع السيبرانية، أو تنفيذها، أو المشاركة فيها.
٢٣	مراجعة وتحليل تهديدات الأمن السيبراني لتزويد أصحاب المصلحة بالمعلومات المطلوبة للاستجابة لهذه التهديدات.
٢٤	تقديم توصيات لتمكين المعالجة الفعّالة للثغرات.
٢٥	دعم القضايا الأمنية لدى الإدارة العليا، والتأكد من شمول الأمن السيبراني ضمن الأهداف الاستراتيجية.
٢٦	تحديد الأدلة الرقمية للفحص والتحليل.
٢٧	إجراء تحليل للبرمجيات الضارة على المستوى الأول والثاني والثالث.
٢٨	استخدام معدات وأساليب مخصصة للقيام بمهام التحقيق الجنائي الرقمي بما يتماشى مع السياسات.
٢٩	استخدام المراجعات للتوصية بتدابير جديدة أو محدثة لجوانب الأمن أو الصمود والموثوقية.
٣٠	تحليل نتائج اختبارات البرمجيات والعتاد والاختبار البيني لتحديد تحسينات ذات كفاءة عالية للحد من المخاطر المكتشفة.
٣١	إعداد وتقديم ملخصات عن تهديدات معينة للجهة.
٣٢	استطلاع الشبكات وتحليل الثغرات للنُظم داخل الشبكة.

#	المسؤوليات
٣٣	إجراء التحليل العقدي الشبكة.
٣٤	الكشف عن حالات الاستغلال ضد الشبكات والمضيفات ذات الاهتمام لإفادة جهود محاولة فهم نشاط ممثل التهديد.
٣٥	تحديد التقنيات المستخدمة من قبل التهديدات ذات العلاقة.
٣٦	تطوير مصادر المعلومات لتعميق فهم التهديدات ذات العلاقة.
٣٧	تطبيق الأساليب التحليلية للحصول على معلومات ممثلي التهديد محل الاهتمام.
٣٨	تقييم عمليات صنع القرار بشأن التهديدات.
٣٩	تحديد التهديدات الأساسية للثغرات المعروفة بالجهة.
٤٠	تقييم القدرات المتوفرة للتصدي لأنشطة التهديدات المحتملة وذلك لتقديم توصية بحلول فعّالة.
٤١	تحديد أساليب التهديد ومنهجياته.
٤٢	تحديد وتقييم القدرات الحرجة للتهديدات، ومتطلباتها وثغراتها.
٤٣	تحديد هيكلة ومكونات ممثل التهديد.
٤٤	تقديم المدخلات أو تطوير مسارات العمل بناء على فهم التهديدات.
٤٥	المراقبة والإبلاغ عن التغيرات في ميول التهديدات وأنشطتها، وأساليبها، وقدراتها، وغاياتها.
٤٦	مراقبة أنشطة التهديد التي تمت مصادقتها والإبلاغ عنها.
٤٧	معالجة الحوادث، وفرز الأحداث حسب أولوياتها، وتحليل الشبكات، وكشف التهديدات، وتحليل التوجهات، وتطوير المقاييس، ونشر المعلومات عن الثغرات.
٤٨	المساندة في تحليل التهديدات والثغرات وتقديم الخدمات والتوصيات الاستشارية في الأمن السيبراني.
٤٩	القيام بتحليل البرمجيات الضارة ذات المستوى الأول والثاني.
٥٠	القيام بأبحاث وعمليات تحليل متعمقة.
٥١	تحديد أساليب ومنهجيات التهديد السيبراني.

مصمم معمارية الأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية (ICS/OT Cybersecurity Architect)

#	المسؤوليات
١	إجراء مراجعات الأمن السيبراني، وتحديد الفجوات في المعمارية الأمنية، من أجل إصدار خطط لإدارة المخاطر السيبرانية.
٢	توفير مدخلات لإطار إدارة المخاطر والوثائق ذات الصلة.
٣	تنفيذ عمليات آمنة لإدارة الإعدادات.
٤	تحديد وظائف الأعمال الحيوية وتصنيف أولوياتها بالتعاون مع أصحاب المصلحة بالجهة.
٥	تقديم استشارات بشأن تكاليف المشاريع، ومفاهيم التصميم التابعة لها، أو التغييرات على تصاميمها.
٦	تقديم المشورة بشأن المتطلبات الأمنية المطلوب إدراجها في وثائق المشتريات.
٧	تحليل المعمارية المرشحة، وتخصيص الخدمات الأمنية واختيار الآليات الأمنية.
٨	تعريف السياق الأمني للنُظم، ومفهوم العمليات واحتياجاتها المبدئية، وفقًا لسياسات الأمن السيبراني المطبقة.
٩	تحرير المواصفات الوظيفية التفصيلية التي توثق عملية تطوير المعمارية.
١٠	تحليل احتياجات المستخدم ومتطلباته لتخطيط المعمارية.
١١	تطوير المعمارية المؤسسية أو مكونات النظام المطلوبة لتلبية احتياجات المستخدم.
١٢	توثيق وتحديث كل أنشطة التعريف والمعمارية، حسب الضرورة.
١٣	تحديد ضوابط الأمن لنظم المعلومات والشبكات، مع توثيقها على نحو ملائم.
١٤	تقييم وتصميم وظائف إدارة الأمن السيبراني.
١٥	تعريف لمستويات التوافر المناسبة لوظائف النظم الحرجة ومتطلبات عمليات التعافي من الكوارث والاستمرارية لتقديمها
١٦	تحديد وتوثيق أثر تنفيذ نظام جديد أو واجهات اتصال جديدة بين النُظم على الوضع الأمني للبيئة الحالية.

#	المسؤوليات
١٧	تقديم التوصيات بخصوص الضوابط الأمنية ذات الكفاءة المالية لمعالجة المخاطر المكتشفة عن طريق الاختبار والمراجعة.
١٨	تحديد وترتيب أولويات قدرات النُظم أو وظائف الأعمال اللازمة لاستعادة النظام جزئيًا أو كليًا بعد وقوع عطل كارثي في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
١٩	تطوير ودمج تصاميم الأمن السيبراني للنُظم والشبكات والتي لها متطلبات أمن متعددة المستويات في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
٢٠	توثيق ومعالجة متطلبات الأمن السيبراني لعمليات النظم، ومتطلبات هندسة الأمن للبُنى المعمارية والنُظم في كافة مراحل عمليات الشراء والاستحواذ في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
٢١	ضمان اتساق النُظم والبُنى المعمارية التي تمت حيازتها أو تطويرها مع إرشادات الجهة لمعمارية الأمن السيبراني في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
٢٢	ترجمة القدرات المقترحة إلى متطلبات تقنية في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
٢٣	العمل مع أعضاء فريق التطوير المرن لتسريع إعداد نماذج أولية ودراسات الجدوى وتقييم التقنيات الحديثة في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
٢٤	تصميم نُظم وحلول لدعم نجاح "حلول إثبات المبدأ" والمشاريع التجريبية في مجالات التقنيات الناشئة في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
٢٥	قراءة وتفسير المخططات والمواصفات والرسومات والتصاميم الأولية والرسومات البيانية التخطيطية ذات العلاقة بالأنظمة والشبكات في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
٢٦	فهم وإصلاح مواطن الخلل في أنظمة الاتصالات والأتمتة الصناعية.
٢٧	تحديد وتوثيق الضوابط الأمنية للأنظمة والشبكات في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.

محلل دفاع الأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية (ICS/OT Cybersecurity Defense Analyst)

#	المسؤوليات
١	ربط بيانات الحوادث لتحديد الثغرات
٢	استخدام منتجات الأمن السيبراني أو تقنيات التحكم الأمني للحد من المخاطر المكتشفة إلى مستويات مقبولة
٣	توثيق وتصعيد الحوادث السيبرانية التي من شأنها أن تؤدي إلى أثر فوري أو مستمر.
٤	تحليل توجهات الدفاع السيبراني، وتقديم تقارير بشأنها
٥	ربط المعلومات من مصادر متعددة للإلمام بالحالة وتحديد فاعلية الهجمة المرصودة
٦	إجراء مراجعات الأمن السيبراني، وتحديد الثغرات الأمنية في المعمارية الأمنية لدعم استراتيجيات معالجة المخاطر
٧	تحليل نتائج التمارين وبيئة النظام للخروج بالتوصيات والتعديلات اللازمة.
٨	تحليل تنبيهات الشبكة التي يتم الحصول عليها من مصادر مختلفة لتحديد الأسباب المحتملة لأي أحداث يتم اكتشافها
٩	الكشف عن الهجمات والأنشطة المشبوهة وحالات إساءة الاستخدام، والتعرف عليها والتنبيه بشأنها في الوقت المناسب، وتمييزها عن الأنشطة الاعتيادية
١٠	تسخير أدوات الدفاع السيبراني للمراقبة المستمرة لأنشطة النظم وتحليلها بهدف تعريف الأنشطة الضارة
١١	تحليل الأنشطة الخبيثة لتحديد الثغرات المستغلة، وأساليب الاستغلال، والتأثيرات على النظم والمعلومات
١٢	تطبيق مبادئ وممارسات الدفاع الأمني متعدد المستويات بما يتماشى مع سياسات الجهة
١٣	تحديد الخطط والأساليب والإجراءات (TTP) لمجموعات التسلل.
١٤	فحص المخططات الشبكية لفهم تدفقات البيانات عبر الشبكة
١٥	التوصية بتصحيحات لثغرات البيئة
١٦	استخدام البيانات الوصفية للتعرف على حالات الاشتباه في حركة مرور البيانات عبر الشبكة وتحليلها
١٧	تحديد المؤشرات والتحذيرات من خلال البحث والتحليل والربط عبر مجموعات بيانات متعددة

#	المسؤوليات
١٨	استخدام أدوات تحليل الحزم للتحقق من تنبيهات نظام كشف التسلل
١٩	عزل البرمجيات الضارة وإزالتها
٢٠	استخدام حركة مرور البيانات عبر الشبكة لتحديد تطبيقات أحد أجهزة الشبكة ونظم التشغيل الخاصة به
٢١	استخدام حركة المرور عبر الشبكات لإعادة تمثيل النشاط الخبيث
٢٢	تحديد عمليات محاولة التعرف على التصميم الشبكي وأنشطة التعرف على أنظمة التشغيل
٢٣	المساعدة في حصر خواص التعرف (التواقيع) لتفعيل استخدامها في أدوات الأمن السيبراني للشبكة وذلك للاستجابة للتهديدات الجديدة والتهديدات التي تمت ملاحظتها سابقًا
٢٤	الإبلاغ عن الحوادث السيبرانية المشتبه بها وفقًا لخطة الجهة للاستجابة للحوادث السيبرانية
٢٥	تحليل التوجهات في الحالة الأمنية للجهة، والإبلاغ عنها
٢٦	تحليل التوجهات في الحالة الأمنية للنُظم، والإبلاغ عنها
٢٧	تقييم مدى كفاية ضوابط التحكم بالوصول بناء على سياسات الجهة
٢٨	مراقبة مصادر البيانات الخارجية للمحافظة على فهم محدث لحالة تهديدات الأمن السيبراني وتحديد القضايا الأمنية التي قد تؤثر على الجهة
٢٩	تقييم ومراقبة جوانب الأمن السيبراني لممارسات الجهة بتطبيق النُظم واختبارها
٣٠	تقديم توصيات الأمن السيبراني للقيادة استنادًا إلى التهديدات والثغرات الجسيمة
٣١	العمل مع أصحاب المصلحة لحل حوادث الأمن السيبراني وقضايا الثغرات في الالتزام
٣٢	تطوير أدوات الدفاع السيبراني
٣٣	وصف وتحليل حركة المرور على الشبكة، لتحديد الأنشطة الشاذة والتهديدات المحتملة لموارد الشبكات
٣٤	التنسيق مع بقية طاقم عمل الدفاع السيبراني للتحقق من مصداقية التنبيهات الشبكية
٣٥	تقديم تقارير مُجملة يومية لأحداث الشبكات والأنشطة الأخرى ذات الصلة بالأمن السيبراني بما يتلاءم مع سياسات ومتطلبات الجهة

أخصائي مخاطر الأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية (ICS/OT Cybersecurity Risk Officer)

#	المسؤوليات
١	التواصل الفعّال مع الإدارة العليا بشأن مخاطر الأمن السيبراني
٢	تطوير أوصاف للمخاطر الأمنية لنظم الحاسب من خلال تقييم التهديدات لتلك النظم وثغراتها
٣	تطوير استراتيجيات للحد من المخاطر من أجل إدارة المخاطر في ظل سياسات الجهة لمستويات المخاطرة المقبولة
٤	تطوير إجراءات مضادة خاصة بالأمن السيبراني واستراتيجيات لمعالجة المخاطر
٥	توصيف مخاطر الأمن السيبراني الأولية أو المتبقية التي تؤثر على تشغيل النظام
٦	التأكد من أن القرارات المتخذة بشأن الأمن السيبراني تستند على المبادئ الأساسية لإدارة المخاطر
٧	أداء مهام الاستجابة للأحداث دعما لفرق الاستجابة للأحداث، شاملا جمع الأدلة الجنائية، وربط حالات التسلل، والتتبع، وتحليل التهديدات ومعالجة الأنظمة
٨	تحليل المخاطر كلما خضع أي برنامج أو نظام لتغيير جوهري
٩	توفير مدخلات لإطار إدارة المخاطر والوثائق ذات الصلة
١٠	ضمان تعريف مخاطر الأمن السيبراني ومعالجتها بالطريقة المناسبة من خلال عملية حوكمة المخاطر للجهة
١١	إجراء تقييم لمخاطر الأمن السيبراني
١٢	مراجعة تدقيقات البرامج والمشاريع السيبرانية، أو تنفيذها، أو المشاركة فيها
١٣	التعاون مع الآخرين لتنفيذ وحفظ برنامج إدارة مخاطر الأمن السيبراني
١٤	انتقاء أفراد وإسناد أدوار محددة لهم فيما يتعلق بتنفيذ إطار إدارة المخاطر

#	المسؤوليات
١٥	وضع استراتيجية إدارة المخاطر بالجهة، شاملة تحديد مستوى تحمل المخاطر
١٦	إجراء تقييم مخاطر أولي لأصول أصحاب المصلحة وتحديث تقييم المخاطر بصفة مستمرة
١٧	العمل مع المسؤولين بالجهة لضمان أن بيانات أدوات المراقبة المستمرة توفر الوعي بمستويات المخاطر القائمة
١٨	استخدام أدوات المراقبة المستمرة لتقييم المخاطر باستمرار
١٩	تقديم توصيات لتمكين المعالجة الفعّالة للثغرات
٢٠	تطوير منهجيات فعّالة لمراقبة وقياس المخاطر، ومدى الالتزام، وجهود توكيد الالتزام
٢١	تنسيق وتقديم الدعم الاستشاري التقني إلى فريق الأمن السيبراني بالجهة لحل حوادث الأمن السيبراني في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية
٢٢	عمل تحليل المخاطر في بيئات أنظمة التحكم الصناعي والتقنيات التشغيلية كلما حدث تغيير في تطبيق أو نظام

أخصائي استجابة للحوادث السيبرانية لأنظمة التحكم الصناعي والتقنيات التشغيلية (ICS/OT Cybersecurity Incident Responder)

#	المسؤوليات
١	ربط بيانات الحوادث لتحديد الثغرات
٢	تحليل السجلات من مصادر متعددة لتحديد التهديدات المحتملة لأمن الشبكة
٣	تحليل أولويات الحوادث لتحديد الثغرة ونطاقها وأولويتها وتأثيرها المحتمل، ومن ثم تقديم توصيات من شأنها توفير العلاج السريع
٤	تحليل توجهات الدفاع السيبراني، وتقديم تقارير بشأنها
٥	إجراء جمع أولي للصور الجنائية بموجب معايير البحث الجنائي ذات العلاقة، وفحصها لتحديد أنسب إجراءات المعالجة

#	المسؤوليات
٦	تحليل تنبيهات الشبكة التي يتم الحصول عليها من مصادر مختلفة لتحديد الأسباب المحتملة لأي أحداث يتم اكتشافها
٧	تتبع الحوادث السيبرانية وتوثيقها منذ اكتشافها إلى حلها النهائي
٨	كتابة ونشر أساليب وإرشادات الدفاع السيبراني وتقارير الأحداث السيبرانية، ومشاركتها مع الجهات ذات العلاقة
٩	تطبيق مبادئ وممارسات الدفاع الأمني متعدد المستويات بما يتماشى مع سياسات الجهة
١٠	جمع آثار التسلل، واستخدام البيانات المكتشفة للحد من حوادث الأمن السيبراني المحتملة داخل الجهة
١١	تحرير ونشر المراجعات للتعلم ولنشر الدروس المستفادة من أحداث الأمن السيبراني
١٢	مراقبة مصادر البيانات الخارجية للمحافظة على فهم محدث لحالة تهديدات الأمن السيبراني وتحديد القضايا الأمنية التي قد تؤثر على الجهة
١٣	تنسيق وظائف الاستجابة للحوادث
١٤	أداء دور الخبير التقني لدعم السلطات القانونية التنفيذية وشرح تفاصيل حادث الأمن السيبراني والتحليل الجنائي، حسب المطلوب
١٥	التنسيق مع محللي معلومات التهديدات السيبرانية بهدف ربط بيانات تقييم التهديدات
١٦	تنسيق وتقديم الدعم الاستشاري التقني إلى فريق الأمن السيبراني بالجهة لحل حوادث الأمن السيبراني في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية
١٧	تنفيذ مهام التعامل الفوري مع حوادث الأمن السيبراني في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية لدعم فريق الاستجابة للحوادث

<رئيس مكتب إدارة البيانات>

#	المسؤوليات
١	التأكد من التزام <مكتب إدارة البيانات> بجميع متطلبات الأمن السيبراني.

#	المسؤوليات
٢	قيادة وتوجيه موظفي <مكتب إدارة البيانات> من خلال الإشراف على التدريب والتوعية والتثقيف بالأمن السيبراني تماشيًا مع مسؤولياتهم.
٣	التأكد من إشراك <مكتب إدارة البيانات> في جميع المسائل الأمنية المتعلقة بالبيانات.
٤	العمل مع <مكتب إدارة البيانات> لتطوير الضوابط الأمنية لحماية البيانات.
٥	الإشراف على سرعة تطبيق التوصيات للتقليل من مخاطر الأمن السيبراني.

موظفو <مكتب إدارة البيانات>

أخصائي الذكاء الاصطناعي للأمن السيبراني (Cybersecurity Artificial Intelligence Specialist)

#	المسؤوليات
١	تطوير عناصر المعمارية الأمنية للحد من التهديدات عند نشوئها.
٢	استخدام لغات برمجة مختلفة لكتابة الشفرات البرمجية ولفتح الملفات، ولقراءتها، ولكتابة المخرجات في ملفات مختلفة.
٣	استخدام لغات مفتوحة المصدر.
٤	تطوير العمليات المؤتمتة وحلول الذكاء الاصطناعي ذوات التصنيف العالمي.
٥	تحديد وتطوير الحلول الحسابية المؤتمتة، شاملا الحلول التحليلية والخوارزمية.
٦	تعزيز الأساليب الإحصائية والتعلُّم الآلي لتحديد الاتجاهات والتحليل التنبئي.
٧	تطبيق المعرفة في التعلّم الآلي، أو الإبصار الحاسوبي (Computer vision)، أو الاستشعار عن بُعد ومعالجة البيانات الكبيرة لأجل معالجة المشاكل المهمة من خلال تطوير البرمجيات لتحديد الخوارزميات والمنهجيات المناسبة.
٨	تحليل البيانات وإجراء تحليل كمي للبيانات باستخدام مجموعة متنوعة من مجموعات البيانات لتحديد العمليات ومراقبتها واستكشافها.

#	المسؤوليات
٩	مواكبة أبحاث الإبصار الحاسوبي (Computer vision) والتعلُّم الآلي لنسخ وتأسيس أساليب جديدة.
١٠	استخدام الأدوات المرئية لتصور البيانات وإنشاء لوحات المعلومات لإيصال النتائج.
١١	تشخيص البيانات وإجراء التحليل الإحصائي والتحليل من خلال التعلّم الآلي.
١٢	استخدام التقنيات الكمية.

مدقق الأمن السيبراني (Cybersecurity Auditor)

#	المسؤوليات
١	الحفاظ على مجموعة أدوات تدقيق الدفاع السيبراني القابلة للتفعيل، بناء على أفضل الممارسات في القطاع، وذلك لدعم عمليات تدقيق الدفاع السيبراني.
٢	إدارة النظم على نظم وبرامج مخصصة للأمن السيبراني.
٣	تحليل المخاطر كلما خضع أي برنامج أو نظام لتغيير جوهري.
٤	إعداد تقارير التدقيق والتقييم التي تحدد النتائج التقنية والإجرائية، وتشمل توصيات بالاستراتيجيات والحلول العلاجية
٥	تتبع نتائج وتوصيات التدقيق لضمان اتخاذ إجراءات معالجة ملائمة.
٦	إدارة معالجة الثغرات بفعالية.
٧	ضمان الحفاظ على سجل تدقيق أدلة التدابير الأمنية.
٨	مراجعة تدقيقات البرامج والمشاريع السيبرانية، أو تنفيذها، أو المشاركة فيها.
٩	الحفاظ المتواصل على المعرفة بالسياسات والتنظيمات ووثائق الالتزام المعمول بها في الأمن السيبراني الدفاعي حسب ما يختص منها بأعمال التدقيق للأمن السيبراني الدفاعي.

#	المسؤوليات
١٠	إجراء أعمال التدقيق للحالة الأمنية للبرامج والشبكة والنظام حسب ما ورد في سياسات الأمن السيبراني، وتقديم توصيات بالأنشطة المطلوبة لعلاج الثغرات المكتشفة.
١١	تطوير عمليات الالتزام الأمني وعمليات تدقيق للخدمات المقدمة من أطراف خارجية.
١٢	المراجعة الدورية لضمان مواءمة سياسات الأمن السيبراني والوثائق ذات العلاقة مع غايات واستراتيجيات الجهة المعلنة.
١٣	ضمان توثيق التصميم والتطوير لأنشطة الأمن السيبراني على نحو ملائم.
١٤	ضمان أن عمليات التدقيق للأمن السيبراني تختبر جميع الجوانب ذات العلاقة بالبنية التحتية للجهة والالتزام بالسياسات.
١٥	تطوير العمليات مع المدققين الخارجيين حول كيفية مشاركة المعلومات بأمان.

أخصائي الخصوصية وحماية البيانات (Privacy/Data Protection Officer)

#	المسؤوليات
١	إجراء تقييمات لمدى التأثير على الخصوصية لضمان حماية سرّية معلومات المعرفات الشخصية بشكل مناسب.
٢	التعاون مع الآخرين بشأن السياسات والعمليات والإجراءات ذات العلاقة بالخصوصية والأمن السيبراني
٣	ضمان وضع الضوابط الملائمة للحد من مخاطر الأمن السيبراني بفاعلية ومعالجة مخاوف الخصوصية خلال عملية تقييم المخاطر.
٤	العمل مع المستشارين القانونيين بالجهة والأطراف الأخرى ذات العلاقة لضمان التزام كافة الخدمات مع متطلبات الخصوصية وأمن البيانات.
٥	العمل مع المستشارين القانونيين والإداريين وأصحاب المصلحة بالجهة لضمان توفر توثيق ملائم للخصوصية والسرية بالجهة والمحافظة عليه.
٦	العمل مع أصحاب المصلحة لتطوير العلاقات مع الجهات التنظيمية والإدارات الحكومية المعنية بقضايا الخصوصية وأمن البيانات.

#	المسؤوليات
٧	ضمان تسجيل كافة مصادر البيانات ومصادر معالجتها لدى سلطات حماية خصوصية البيانات حسب اللزوم.
٨	العمل مع فرق الأعمال والإدارة العليا لضمان التوعية بأفضل الممارسات في مجال خصوصية المعلومات وأمن البيانات.
٩	العمل مع الإدارة العليا بالجهة لتأسيس لجنة مراقبة لخصوصية البيانات.
١٠	توفير القيادة في اللجنة المسؤولة عن مراقبة خصوصية البيانات.
١١	تطوير وتوثيق إجراءات بلاغات الإفصاح الذاتي عن أية أدلة على انتهاكات الخصوصية.
١٢	العمل كحلقة اتصال لخصوصية المعلومات لمستخدمي الأنظمة التقنية، والإبلاغ عن الخروقات للإدارة العليا.
١٣	تطوير مواد التدريب والاتصالات الأخرى لزيادة فهم الموظفين لسياسات الخصوصية بالجهة وممارسات معالجة البيانات والالتزامات القانونية.
١٤	الإشراف على التدريب والتعريف الأولي في مجال الخصوصية، وتوجيهه وضمان تقديمه لكل من الموظفين والمتطوعين والمقاولين والحلفاء وشركاء العمل وأيّ أطراف أخرى ذات صلة.
١٥	ضمان تقديم التدريب والتوعية بالخصوصية بصفة دورية.
١٦	العمل مع الشؤون الخارجية لتطوير العلاقات مع منظمات المستهلكين وغيرها من المنظمات غير الحكومية المهتمة بقضايا الخصوصية وأمن البيانات.
١٧	العمل مع إدارة الجهة والمستشارين القانونيين والأطراف الأخرى ذات الصلة لتمثيل مصالح خصوصية المعلومات للجهة أمام الأطراف الخارجية.
١٨	تقديم التقارير الدورية عن الوضع الراهن لبرنامج الخصوصية لصالح الإدارة العليا أو المسؤولين أو اللجان الآخرين.
١٩	توفير القيادة لبرنامج الخصوصية بالجهة.
٢٠	توجيه مسؤولي الخصوصية والإشراف على أعمالهم، وتنسيق برامج الخصوصية وأمن البيانات مع الإدارة العليا لضمان التناسق عبر الجهة.
٢١	ضمان الالتزام بممارسات الخصوصية عبر الجهة.

#	المسؤوليات
٢٢	العمل مع فرق الموارد البشرية والقانونية لتطوير عقوبات مناسبة لعدم الالتزام بسياسات وإجراءات الخصوصية للجهة
٢٣	حلّ مزاعم عدم الالتزام بسياسات الخصوصية للجهة، أو ممارسات إبلاغ المعلومات، دون تأخر.
٢٤	تطوير وحفظ إطار خصوصية لإدارة المخاطر وضمان الالتزام.
٢٥	مراجعة مشاريع البيانات والخصوصية بالجهة وضمان التزامها بسياسات الخصوصية وأمن البيانات بالجهة.
٢٦	إنشاء عملية لإدارة جميع جوانب الشكاوى المتعلقة بسياسات وإجراءات الخصوصية في الجهة.
٢٧	توفير القيادة في أعمال التخطيط والتصميم والتقييم للمشاريع ذات الصلة بالخصوصية والأمن السيبراني.
٢٨	إنشاء ومتابعة برنامج تدقيق داخلي للخصوصية.
٢٩	المراجعة الدورية لبرنامج الخصوصية وتحديثه ليشمل التغييرات في القوانين أو الأنظمة أو سياسة الجهة.
٣٠	تقديم إرشادات التطوير والمساعدة فيما يخص سياسات وإجراءات خصوصية المعلومات بالجهة.
٣١	ضمان أن استخدام التقنيات يحافظ على سُبل حماية الخصوصية، سواء عند الاستخدام أو الجمع أو الإفصاح عن المعلومات الشخصية، ولا يؤدي إلى تعريتها.
٣٢	مراقبة تطوير النُظم وعملياتها لضمان التزامها بسياسات الخصوصية والأمن.
٣٣	إجراء تقييمات للآثار المترتبة على الخصوصية جراء قواعد جديدة مقترحة في حق خصوصية المعلومات الشخصية.
٣٤	مراجعة كافة خطط الأمن السيبراني لضمان المواءمة بين الأمن السيبراني وممارسات الخصوصية.
٣٥	تطوير وإدارة إجراءات التمحيص وتدقيق الموردين للالتزام بالمتطلبات المناسبة في مجالات الخصوصية وأمن البيانات والمتطلبات القانونية والتنظيمية
٣٦	التأكد من أن كافة الشكاوى ذات العلاقة بسياسة الخصوصية للجهة والوثائق ذات العلاقة تتم معالجتها دون تأخر من خلال المورد المناسب
٣٧	تحديد وعلاج الفجوات في التزام الجهة بمتطلبات الخصوصية.

#	المسؤوليات
٣٨	التنسيق مع رئيس إدارة الأمن السيبراني أو من يقوم بعمله لضمان المواءمة بين ممارسات الأمن السيبراني وممارسات الخصوصية.
٣٩	إعداد الاتصالات والتدريبات المناسبة لتحفيز وتعليم كافة الموظفين، بما فيهم القيادات العليا، فيما يخص الالتزام بالخصوصية وعواقب عدم الالتزام، والمداومة على ذلك.
٤٠	ضمان أداء أنشطة مراقبة الالتزام بالخصوصية بصفة مستمرة.
٤١	ضمان تسخير التقنيات الملائمة لاستمرار التزام الجهة بمتطلبات الخصوصية.
٤٢	تطوير خطط استراتيجية مع الإدارة العليا لضمان معالجة المعلومات الشخصية وفقًا لمتطلبات الخصوصية المعمول بها.
٤٣	تطوير إجراءات على مستوى الجهة ومتابعتها لضمان تطوير المنتجات والخدمات الجديدة بما يتسق مع سياسات الخصوصية بالجهة والتزاماتها القانونية.
٤٤	العمل مع رئيس إدارة الأمن السيبراني والمستشار القانوني والإدارة العليا لإدارة حوادث وانتهاكات الخصوصية وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.
٤٥	المحافظة على التوعية بقوانين الخصوصية وأنظمتها ومعايير الاعتماد المعمول بها.

<رئيس الإدارة المعنية بتقنية المعلومات>

#	المسؤوليات
١	التأكد من التزام <الإدارة المعنية بتقنية المعلومات> بجميع متطلبات الأمن السيبراني.
٢	قيادة وتوجيه موظفي <الإدارة المعنية بتقنية المعلومات> من خلال الإشراف على التدريب والتوعية والتثقيف بالأمن السيبراني تماشيًا مع مسؤولياتهم.
٣	المشاركة والمساهمة في تطوير إطار وإجراءات وعمليات إدارة المخاطر وتطبيقها.
٤	اعتماد وسائل يدوية (غير آلية) للتحديثات والإصلاحات في حال لم تكن الأدوات الآلية المستخدمة في <اسم الجهة> مدعومة.

#	المسؤوليات
٥	الإشراف والمتابعة الدورية لتنفيذ الحلول الآلية لإدارة حزم التحديثات والإصلاحات.
٦	مراجعة فاعلية وكفاءة إدارة التحديثات والإصلاحات في الأنظمة الحساسة المتعلقة بتقنية المعلومات.
٧	التأكد من إشراك <الإدارة المعنية بالأمن السيبراني> في جميع المسائل الأمنية المتعلقة بالأصول المعلوماتية والتقنية، وإدارة المشاريع، والمشتريات.
٨	التأكد من إشراك <الإدارة المعنية بالأمن السيبراني> لضمان حماية الأصول المعلوماتية والتقنية لـ<اسم الجهة> على النحو المطلوب.
٩	التأكّد من مراجعة عقود الصيانة الحالية مع موردي أنظمة تقنية المعلومات و/أو الأنظمة الحسّاسة لتزويد <اسم الجهة> بأحدث الإصدارات من حزم التحديثات والإصلاحات.
١٠	الإشراف على سرعة تطبيق التوصيات للتقليل من مخاطر الأمن السيبراني.
١١	الإشراف على إدارة عمليات التشغيل للأصول التقنية المتعلقة بالأمن السيبراني.

موظفو <الإدارة المعنية بتقنية المعلومات>

#	المسؤوليات
١	تطبيق متطلبات الأمن السيبراني المتعلقة ب<الإدارة المعنية بتقنية المعلومات>، بما في ذلك سياسات الأمن السيبراني وإجراءاته، وعملياته ومعاييره وإرشاداته.
٢	معالجة الثغرات ومتابعة تطبيق حزم التحديثات الأمنية والإعدادات.
٣	تطبيق متطلبات الأمن السيبراني فيما يتعلق بطبيعة عمل الموظف المعني.
٤	تصعيد أي أنشطة مشبوهة أو مخاوف تتعلق بالأمن السيبراني إلى <الإدارة المعنية بالأمن السيبراني> والإبلاغ عنها.
٥	المساعدة في تقديم مدخلات لأنشطة عمليات إطار إدارة المخاطر والوثائق ذات العلاقة.
٦	التنسيق مع <الإدارة المعنية بالأمن السيبراني> حول جميع المسائل المتعلقة بالأصول المعلوماتية والتقنية وإدارة المشاريع.
٧	التنسيق مع <الإدارة المعنية بالأمن السيبراني> لضمان حماية الأصول المعلوماتية والتقنية لـ<اسم الجهة> وتأمينها على النحو المطلوب.

٨	مراجعة عقود الصيانة الحالية مع موردي أنظمة تقنية المعلومات والأنظمة الحسّاسة للتأكد من تزويد <اسم الجهة> بأحدث الإصدارات من حزم التحديثات والإصلاحات.

الأدوار والمسؤوليات الخاصة ب<أمن تقنية المعلومات>

أخصائي تطوير أمن النظم (Systems Security Development Specialist)

#	المسؤوليات
١	تطبيق السياسات الأمنية على التطبيقات المتداخلة بين بعضها البعض.
٢	تطوير أوصاف للمخاطر الأمنية لنظم الحاسب من خلال تقييم التهديدات لتلك النظم وثغراتها.
٣	إجراء تقييمات لمدى التأثير على الخصوصية لضمان حماية سرّية معلومات المعرفات الشخصية بشكل مناسب.
٤	تطوير استراتيجيات للحد من المخاطر من أجل إدارة المخاطر بالتوافق مع سياسات الجهة لمستويات المخاطرة المقبولة.
٥	تطوير تدابير مضادة خاصة بالأمن السيبراني واستراتيجيات لمعالجة المخاطر.
٦	التأكد من أن أي منتج يتم استخدامه لإدارة مخاطر الأمن السيبراني تم تقييمه بفعالية والتصريح باستخدامه.
٧	تحليل المخاطر السيبرانية كلما خضع أي برنامج أو نظام لتغيير جوهري.
٨	توفير مدخلات لإطار إدارة المخاطر والوثائق ذات الصلة.
٩	تصميم ضوابط وإجراءات أمن النُظم التي توفر السرية والسلامة والتوافر والتحقق وعدم الإنكار، وتطويرها وتحقيق تكاملها وتحديثها.
١٠	إجراء تقييم لمخاطر الأمن السيبراني.
١١	توفير الخبرة المتخصصة لتطوير وهندسة الجيل القادم من الأمن السيبراني.
١٢	تحديد وظائف الأعمال الحيوية وتصنيف أولوياتها بالتعاون مع أصحاب المصلحة بالجهة.
١٣	تحليل قيود التصميم والمفاضلات في التصميم التفصيلي للأمن السيبراني للنظام مع الأخذ في الاعتبار دعم دورة حياة النظام.
١٤	تقييم فاعلية تدابير الأمن السيبراني للنظم.

#	المسؤوليات
١٥	بناء نماذج أولية للمنتجات واختبارها وتعديلها، لإثبات على التزامها بمتطلبات الأمن السيبراني، وذلك من خلال النماذج الفعلية أو النظرية.
١٦	تصميم وتطوير الأمن السيبراني أو المنتجات المدعومة بالأمن السيبراني.
١٧	تصميم العتاد ونُظم التشغيل وتطبيقات البرمجيات لتلبية متطلبات الأمن السيبراني.
١٨	تصميم أو دمج النسخ الاحتياطي الآمن، والتخزين المحمي لقدرات النسخ الاحتياطية للبيانات، حسب المناسب في التصاميم.
١٩	تطوير وتوجيه الإجراءات وأعمال التوثيق لعمليات اختبار النظم وعمليات المصادقة.
٢٠	تطوير وثائق التصميم الأمني التفصيلية بخصوص مواصفات المكونات والواجهات لدعم تصميم النظام وتطويره.
٢١	تطوير واختبار خطط التعافي من الكوارث واستمرارية العمليات للنُظم الخاضعة للتطوير وذلك قبل إدخال النظم في بيئة الإنتاج الحية.
٢٢	تحديد وتخصيص الوظائف الأمنية للمكونات، ووصف العلاقات بينها.
٢٣	تحديد وتوجيه معالجة المشكلات التقنية التي تتم مواجهتها في أثناء اختبار وتنفيذ نُظم جديدة.
٢٤	ضمان تضمين الأمن السيبراني بداخل عمليات تطوير البرامج، وحفظها، وإخراجها من الخدمة.
٢٥	ضمان إدراج تنبيهات الثغرات الأمنية في تصاميم النظام.
٢٦	إدارة تجميع البيانات، وفهرستها، والتخزين المؤقت لها، وتوزيعها واسترجاعها.
٢٧	تقديم إرشادات لتنفيذ النظم المطورة للعملاء أو فرق التركيب.
٢٨	تقديم دعم لاختبارات الترخيص الأمنية وأنشطة التقييم.
٢٩	استخدام النماذج والمحاكاة لتحليل أداء النظام في ظل ظروف تشغيل مختلفة أو التنبؤ به.
٣٠	تصميم وتطوير وظائف إدارة الأمن السيبراني الرئيسية.
٣١	تحليل احتياجات ومتطلبات المستخدمين للتخطيط لأمن النظام وتطويره.
٣٢	تطوير تصاميم الأمن السيبراني لتلبية احتياجات تشغيلية وعوامل بيئية محددة.
٣٣	تنفيذ منهجيات دورة حياة تطوير النظام ودمجها في بيئة التطوير لأنظمة الأمن السيبراني.

#	المسؤوليات
٣٤	توظيف عمليات إدارة الإعدادات عند تطبيق أنظمة الأمن السيبراني.
٣٥	تصميم الواجهات الآمنة بين نُظم المعلومات والنُظم المادية والتقنيات المدمجة، وتنفيذها واختبارها وتقييمها.
٣٦	التصميم حسب المتطلبات الأمنية، لضمان تلبية المتطلبات لجميع النُظم والتطبيقات.
٣٧	وضع استراتيجيات المعالجة لمواجهة المخاطر ذات الصلة بالتكلفة والجداول الزمنية والأداء والأمن.
٣٨	إجراء المراجعات الأمنية وتحديد الفجوات الأمنية في البنية المعمارية.
٣٩	تقديم المدخلات للخطط التنفيذية لأمن أنظمة المعلومات وإجراءات التشغيل النمطية.
٤٠	تتبع متطلبات النظام لتصميم المكونات وإجراء تحليل الفجوة.
٤١	التحقق من أن معمارية النظام مستقرة، وتحقق التشغيل البيني (interoperability)، وقابلة للنقل، وقابلة للتوسع.
٤٢	ضمان توثيق التصميم والتطوير لأنشطة الأمن السيبراني على نحو ملائم.

أخصائي البنية التحتية للأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية (ICS/OT Cybersecurity Infrastructure Specialist)

#	المسؤوليات
١	تطبيق السياسات الأمنية لتحقيق الأهداف الأمنية للنظام.
٢	إدارة النظم على نظم وبرامج مخصصة للأمن السيبراني.
٣	تحديد حماية البنية التحتية الحاسمة للدفاع السيبراني ومواردها، وترتيب أولوياتها وتنسيقها.
٤	تطبيق وظائف الأمن السيبراني (مثل التشفير والتحكم في الوصول وإدارة الهوية) لتقليل فرص الاستغلال.
٥	الإدارة والإشراف على أعمال تحديث القواعد والتواقيع لتطبيقات الدفاع السيبراني.
٦	إعداد وتهيئة برامج وأجهزة تعزيز الأمن السيبراني المخصصة، وتثبيتها، وتحديثها، واختبارها.
٧	المساعدة في تقييم أثر بناء وتشغيل بنية تحتية مخصصة تعزيز الأمن السيبراني.

#	المسؤوليات
٨	إدارة منصات الاختبار، واختبار وتقييم التطبيقات وأجهزة البنية التحتية والقواعد والتوقيعات، وضوابط التحكم بالوصول وإعدادات المنصات التي يديرها مزودو الخدمات.
٩	إنشاء قوائم التحكم بالوصول إلى الشبكات المخزنة بداخل نُظم الدفاع السيبراني المخصصة، وتعديلها وإدارتها.
١٠	تحديد التعارضات المحتملة جراء تنفيذ أي من أدوات الدفاع السيبراني، والإبلاغ عنها.
١١	تنفيذ متطلبات إطار إدارة المخاطر والتقييم الأمني والتصريح لنُظم الدفاع السيبراني المخصصة داخل الجهة، وتوثيق سجلاتها وحفظها.
١٢	تحديد ضوابط الأمن السيبراني للنظام وتوثيق الوصف الوظيفي لتنفيذ الضوابط في الخطة الأمنية.
١٣	تنفيذ ضوابط الأمن السيبراني الواردة في الخطة الأمنية أو وثائق النُظم الأخرى.
١٤	تطوير العمليات والإجراءات الخاصة بالتحديث وعمل تحديث الإصلاح اليدوي لبرمجيات النُظم بحسب متطلبات الجدول الزمني الحالي أو المتوقع لتطبيق حزم تحديثات الإصلاح على البيئة التشغيلية للنظام.
١٥	انتقاء ضوابط الأمن السيبراني للنظام وتوثيق الوصف الوظيفي لتنفيذ الضوابط في الخطة الأمنية في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
١٦	تنفيذ ضوابط الأمن السيبراني الواردة في الخطة الأمنية أو وثائق النُظم الأخرى في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
١٧	فهم وإصلاح مواطن الخلل في أنظمة الاتصالات والأتمتة الصناعية.

محلل أمن النظم (Systems Security Analyst)

#	المسؤوليات
١	تطبيق السياسات الأمنية على التطبيقات المتداخلة بين بعضها البعض.
٢	تطبيق السياسات الأمنية لتحقيق الأهداف الأمنية للنظام.

#	المسؤوليات
٣	استخدام منتجات الأمن السيبراني أو تقنيات التحكم الأمني للحد من المخاطر المكتشفة إلى مستويات مقبولة.
٤	إجراء مراجعات الأمن السيبراني، وتحديد الفجوات في المعمارية الأمنية، من أجل إصدار خطط لإدارة المخاطر السيبرانية.
٥	تحليل نتائج التمارين وبيئة النظام للتخطيط وللتوصية بتعديلات وتسويات.
٦	توفير مدخلات لإطار إدارة المخاطر والوثائق ذات الصلة.
٧	مراجعة وثائق الأمن السيبراني العاكسة لتصميم النظام، وتحديثها وحفظها.
٨	تقييم فاعلية ضوابط الأمن السيبراني.
٩	تقييم عملية إدارة الإعدادات.
١٠	تحليل التوجهات في الحالة الأمنية للجهة، والإبلاغ عنها.
١١	تحليل التوجهات في الحالة الأمنية للنُظم، والإبلاغ عنها.
١٢	تقييم مدى كفاية ضوابط التحكم بالوصول بناء على سياسات الجهة.
١٣	تقييم ومراقبة جوانب الأمن السيبراني لممارسات الجهة بتطبيق النُظم واختبارها.
١٤	تقديم توصيات الأمن السيبراني للقيادة استنادًا إلى التهديدات والثغرات الجسيمة.
١٥	العمل مع الأطراف المعنيين لحل حوادث الأمن السيبراني وقضايا الثغرات في الالتزام.
١٦	تحديد وتخصيص الوظائف الأمنية للمكونات، ووصف العلاقات بينها.
١٧	تطبيق مبادئ المعمارية الأمنية الموجهة للخدمات لاستيفاء متطلبات الجهة الخاصة بالسرية والسلامة والتوافر.
١٨	ضمان توثيق جميع عمليات أمن النُظم وأنشطة الصيانة على نحو ملائم، وتحديثها حسب الضرورة.
١٩	تطبيق التحديثات وحزم التحديثات الأمنية للمنتجات التجارية بما يتوافق مع الأطر الزمنية التي تمليها السلطة الإدارية فيما يخص بيئة التشغيل المعنية.
٢٠	تنفيذ تدابير أمن سيبراني مضادة محددة للنظم والتطبيقات.

#	المسؤوليات
٢١	دمج القدرات المؤتمتة المخصصة لتحديث أو عمل تحديثات إصلاح برمجيات النظام، حيثما أمكن ذلك عمليا.
٢٢	ضمان اختبار الأمن السيبراني للتطبيقات والنظم بعد تطويرها.
٢٣	توثيق وتحديث جميع الأنشطة المتعلقة بتنفيذ وتشغيل وصيانة أمن الأنظمة.
٢٤	تقديم إرشادات بشأن الأمن السيبراني إلى الإدارة المعنية بالأمن السيبراني.
٢٥	تطوير واختبار إجراءات نقل عمليات النظام إلى موقع بديل.
٢٦	تنفيذ إجراءات التعافي من الكوارث واستمرارية الأعمال.
٢٧	تنفيذ تدابير أمنية على النظام أو مكونات النظام لمعالجة الثغرات وتقليل المخاطر، والتوصية بعمل تغييرات تتعلق بالأمن السيبراني.
٢٨	تنفيذ التدابير والضوابط الأمنية للنظام وفقًا للإجراءات المعمول بها.
٢٩	ضمان دمج وتنفيذ الحلول العابرة للنطاقات في بيئة آمنة.
٣٠	رفع التوصيات للإدارة بعمل الإجراءات اللازمة للمعالجة والتصحيح أو بقبول المخاطر الناتجة عن جوانب القصور الأمني التي يتم اكتشافها عند الفحص.
٣١	التحقق من وجود الحد الأدنى من المتطلبات الأمنية لجميع التطبيقات.
٣٢	تطوير العمليات والإجراءات الخاصة بالتحديث وعمل تحديث الإصلاح اليدوي لبرمجيات النُظم بحسب متطلبات الجدول الزمني الحالي أو المتوقع لتطبيق حزم تحديثات الإصلاح على البيئة التشغيلية للنظام.

أخصائي إدارة الهوية والوصول (Identity and Access Management Specialist)

#	المسؤوليات
١	تقييم مدى كفاية ضوابط التحكم بالوصول بناء على سياسات الجهة.
٢	تطبيق وظائف الأمن السيبراني (مثل التشفير والتحكم في الوصول وإدارة الهوية) لتقليل فرص الاستغلال.

#	المسؤوليات
٣	تطوير تصاميم الأمن السيبراني لتلبية احتياجات تشغيلية وعوامل بيئية.
٤	إنشاء قوائم التحكم بالوصول إلى الشبكات المخزنة بداخل نُظم تعزيز الأمن السيبراني المخصصة، وتعديلها وإدارتها.
٥	العمل مع الفرق الأخرى لتصميم وتطوير وتأمين حلول لإدارة الهوية والوصول.
٦	العمل مع معماري الأمن السيبراني لتطوير استراتيجية إدارة الهوية والوصول.
٧	ضمان اتباع معايير وسياسات الجهة عند تنفيذ حلول إدارة الهوية والوصول.
٨	العمل مع الأطراف المعنية لتحديد ومعالجة الثغرات عند تنفيذ حلول إدارة الهوية والوصول.
٩	تقديم التوجيه والنصيحة إلى أعضاء الفريق بشأن أنظمة إدارة الهوية والوصول وعملياتها.
١٠	إعداد سياسات المجموعات وقوائم التحكم في الوصول لضمان التوافق مع المعايير التنظيمية وقواعد العمل والاحتياجات.
١١	إدارة الحسابات وصلاحيات الشبكة والوصول إلى الأنظمة والمعدات.
١٢	تصميم وتطوير وظائف إدارة النظم والإشراف عليها للمستخدمين ذوي الصلاحيات الإضافية.
١٣	الإشراف على الحسابات وصلاحيات الشبكة والوصول إلى الأنظمة والمعدات.
١٤	إعداد عمليات وإجراءات التحكم في الوصول لأدوات وتقنيات المراقبة المستمرة.
١٥	ضمان أن تتم إدارة الوصول لأدوات وتقنيات المراقبة المستمرة بشكل مناسب.

أخصائي التشفير (Cryptography Specialist)

#	المسؤوليات
١	فك تشفير البيانات المضبوطة باستخدام وسائل تقنية.
٢	التأكد من توافق قدرات الاكتشاف والحماية السيبرانية مع استراتيجية وسياسات الأمن السيبراني للجهة، ومع المستندات الأخرى ذات العلاقة.

#	المسؤوليات
٣	تطوير قدرات إدارة البيانات الآمنة لدعم القوى العاملة المتنقلة.
٤	تمكين التطبيقات بالمفاتيح العامة من خلال مكتبات البنية التحتية للمفاتيح العمومية القائمة، مع تضمين إدارة الشهادات والتشفير حسب الحاجة.
٥	تصميم ضوابط وإجراءات أمن النُظم التي توفر السرية والسلامة والتوافر والتحقق وعدم الإنكار، وتطويرها، وتحقيق تكاملها وتحديثها.
٦	تطبيق وظائف الأمن السيبراني (مثل التشفير والتحكم في الوصول وإدارة الهوية) لتقليل فرص الاستغلال.
٧	تطبيق مبادئ المعمارية الأمنية الموجهة للخدمات لاستيفاء متطلبات الجهة الخاصة بالسرية والسلامة والتوافر.
٨	الكشف عن البيانات المشفرة والمخفية وتحليلها.
٩	تنفيذ التدابير والضوابط الأمنية للنظام وفقًا للإجراءات المعمول بها.
١٠	تطوير خوارزميات التشفير وتصميمها وتنفيذها لتفي بمتطلبات الجهة.
١١	تحليل خوارزميات التشفير للكشف عن نقاط ضعفها وكسر الشفرات.

مطور الأمن السيبراني (Cybersecurity Developer)

#	المسؤوليات
١	أداء البرمجة الآمنة وتحديد مواطن الخلل المحتملة في الشفرات البرمجية لمعالجة الثغرات.
٢	تحليل المخاطر كلما خضع أي برنامج أو نظام لتغيير جوهري.
٣	تحليل نتائج التمارين وبيئة النظام للتخطيط وللتوصية بتعديلات وتسويات.
٤	تمكين التطبيقات بالمفاتيح العامة من خلال مكتبات البنية التحتية للمفاتيح العمومية القائمة، مع تضمين إدارة الشهادات والتشفير حسب الحاجة.
٥	تطبيق وظائف الأمن السيبراني (مثل التشفير والتحكم في الوصول وإدارة الهوية) لتقليل فرص الاستغلال.

#	المسؤوليات
٦	تحليل المعلومات لتحديد متطلبات التطوير لبرنامج جديد أو تعديل برنامج قائم، والتوصية والتخطيط في ذلك كله.
٧	تحليل كيفية تلبية احتياجات المستخدم ومتطلبات البرمجيات بما يتماشى مع سياسات الأمن السيبراني، وتحديد مدى واقعية التصميم، ضمن القيود الزمنية والمالية.
٨	تطبيق معايير الأمن للبرمجة والاختبار.
٩	توثيق الشفرات البرمجية الآمنة.
١٠	دمج الأمن السيبراني في عملية المتطلبات عن طريق تعريف الضوابط الأمنية وتوثيقها.
١١	ضمان توثيق سير تطوير البرامج وتحديثها، وضمان قدرة الآخرين على فهمها من خلال إدراج التعليقات في الشفرات البرمجية.
١٢	تحديد قيود المشاريع، وقدراتها، ومتطلبات أدائها، ومواطن ارتباطها.
١٣	تقييم مواطن الارتباط بين العتاد والبرامج من خلال الاستشارة مع الكوادر الهندسية.
١٤	العمل على ضمان الحصول على النتائج المرجوة من خلال إعادة التحقق من البرنامج وإجراء التغييرات المناسبة لتصحيح الأخطاء.
١٥	تطوير عمليات البرمجة الآمنة وعمليات التعامل مع الأخطاء، وتوثيقهما.
١٦	تطبيق المنهجيات لإصلاح الأخطاء البرمجية الشائعة ذات التبعات الأمنية لضمان تطوير برمجيات آمنة.
١٧	ضمان تضمين الأمن السيبراني بداخل عمليات تطوير البرامج، وحفظها، وإخراجها من الخدمة.
١٨	إجراء اختبارات مدمجة لضمان جودة وظائف الأنظمة الأمنية وصمودها.
١٩	إعداد مخططات تدفق العمليات والرسومات البيانية التي توضح المدخلات والمخرجات والعمليات المنطقية للأنظمة الأمنية.
٢٠	معالجة التبعات الأمنية في مرحلة قبول البرمجيات.
٢١	ترجمة المتطلبات الأمنية إلى عناصر تصميم التطبيق، بما في ذلك توثيق عناصر الأجزاء المعرضة للهجوم في البرمجيات وتصميم نماذج للتهديدات وتحديد أي ضوابط أمنية خاصة.
٢٢	استشارة العملاء بخصوص تصميم أنظمة الأمن السيبراني وصيانتها.

#	المسؤوليات
٢٣	توجيه أعمال البرمجة لتطبيقات الأمن السيبراني وأعمال تطوير مستنداتها التوثيقية.
٢٤	استخدام لغات برمجة مختلفة لكتابة الشفرات البرمجية ولفتح الملفات، ولقراءتها، ولكتابة المخرجات في ملفات مختلفة.
٢٥	تحديد العمليات والخدمات الأمنية المؤسسية عند تصميم وتطوير التطبيقات الآمنة، والاستفادة منها.
٢٦	التشغيل التجريبي للبرامج وتطبيقات البرمجيات، لضمان إنتاج المعلومات المرغوبة، وضمان سلامة التعليمات والمستويات الأمنية.
٢٧	تطوير إجراءات اختبار النظام ومصادقتها، والبرمجة والتوثيق.
٢٨	تعديل البرمجيات القائمة وحفظها لتصحيح الأخطاء أو تكييفها مع أجهزة جديدة أو ترقية الواجهات وتحسين الأداء.
٢٩	تحديد وتوثيق حزم تحديثات الإصلاح للبرمجيات أو نطاق الإصدارات الذي سينشأ عنه ثغرات بالبرامج.
٣٠	ابتكار أساليب وحلول إبداعية مخصصة للاستغلال لاكتشاف الثغرات ومدى عُرضة الأهداف لأعمال الاستغلال.

<مسؤول تطوير التطبيقات>

#	المسؤوليات
١	الإشراف على تنفيذ متطلبات الأمن السيبراني المتعلقة بتطوير التطبيقات في <اسم الجهة>.
٢	التنسيق مع فريق الأمن السيبراني حول المسائل المتعلقة بالأمن السيبراني التي تؤثر على <الإدارة المعنية بتطوير التطبيقات>.
٣	التأكد من تطبيق معايير الأمن السيبراني المعتمدة لتطوير التطبيقات، مثل (Open Web Application Security Project “OWASP”).
٤	الإشراف على تطبيق معايير وأدوات الاختبار الأمني (Testing Standards) والمعايير الأمنية لشفرة البرامج والتطبيقات (Coding Standards)، بما في ذلك الفحص العشوائي (Fuzzing)

#	المسؤوليات
	لأدوات التحليل الثابت للشفرات (Static Code Analysis) وإجراء مراجعات لشفرة البرامج والتطبيقات (Code Reviews).)
٥	تحديد حزم التحديثات والإصلاحات وتوثيقها والتأكد من سلامتها قبل تنصيبها.
٦	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.
٧	التأكد من البرمجة الآمنة من خلال التأكد من معالجة الأخطاء وتحديد الأخطاء المحتملة في التشفير للحد من الثغرات.
٨	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.
٩	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:
١	تنفيذ متطلبات الأمن السيبراني المتعلقة بتطوير التطبيقات في <اسم الجهة>، واتباع المعايير والإجراءات المعتمدة في تطوير التطبيقات (مثل: معايير التطوير الآمن للتطبيقات).
٢	متابعة عمليات إدارة المشاريع والتغييرات في <اسم الجهة>، وذلك بالنسبة لجميع التغييرات التي تنطبق على التطبيقات الخاصة ب<اسم الجهة>.
٣	تحديد التحديثات والإصلاحات اللازمة للبرامج وتوثيقها.
٤	إجراء البرمجة الآمنة، ومعالجة الأخطاء، وتحديد الأخطاء المحتملة في التشفير للحد من الثغرات.

#	المسؤوليات
٥	تطبيق معايير وأدوات الاختبار الأمني والمعايير الأمنية لشفرة البرامج والتطبيقات، بما في ذلك الفحص العشوائي لأدوات التحليل الثابت للشفرات، وإجراء مراجعات لشفرة البرامج والتطبيقات.
٦	تحديد وتوثيق التحديثات والإصلاحات اللازمة للبرامج، والإصدارات التي تكون خلالها البرامج عرضة للثغرات.

<مسؤول عمليات تقنية المعلومات>

#	المسؤوليات
١	تنسيق فترات الصيانة حسب الأولوية وتخطيطها وتحديد موعدها من أجل تثبيت التحديثات والإصلاحات وفقًا لسياسة إدارة المشاريع والتغييرات المعتمدة في <اسم الجهة> بما لا يؤثر على الأمن السيبراني للأصول.
٢	الإشراف على الحلول الآلية لإدارة حزم التحديثات والإصلاحات، والتأكد من إجراء التحديثات اليدوية في حال كانت التحديثات والإصلاحات الآلية غير مدعومة.
٣	الإشراف على النسخ الاحتياطية المنتظمة واختبارات النسخ الاحتياطية.
٤	الإشراف على تنفيذ متطلبات الأمن السيبراني المتعلقة بعمليات تقنية المعلومات في <اسم الجهة>.
٥	التأكد من اختبار تحديثات وإصلاحات الأصول المعلوماتية والتقنية قبل النشر.
٦	التأكد من نجاح تثبيت التحديثات والإصلاحات على الأنظمة.
٧	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).
٨	تحديد وترتيب الأولويات والقدرات لاستعادة الأنظمة ووحدات الأعمال الأساسية اللازمة كليًا أو جزئيًا بعد وقوع حدث كارثي يؤثر على الأنظمة واستمرارية الأعمال.
٩	تحديد المستويات الملائمة لتوافر المعلومات في الأنظمة، وذلك استنادًا 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 واسترداد النظام.

#	المسؤوليات
١٠	الإشراف على اختبار كفاءة خطة التعافي من الكوارث والمشاركة في اختبار كفاءة خطة استمرارية الأعمال.

موظفي تقنية المعلومات

#	المسؤوليات
	بالإضافة إلى جميع المسؤوليات المذكورة لموظفي <الإدارة المعنية بتقنية المعلومات>، يتولّى المعنيون بعمليات تقنية المعلومات المسؤوليات التالية:
١	المساعدة في التنسيق مع <الإدارة المعنية بالأمن السيبراني> حول المسائل المتعلقة بالأمن السيبراني التي تؤثر على الإدارة المعنية بعمليات تقنية المعلومات.
٢	تنفيذ متطلبات الأمن السيبراني المتعلقة بعمليات تقنية المعلومات في <اسم الجهة>.
٣	تنفيذ الحلول الآلية لإدارة حزم التحديثات والإصلاحات.
٤	القيام بعمل نسخ احتياطية واختبارها دوريًا.
٥	تنفيذ الحلول الآلية لإدارة حزم التحديثات والإصلاحات، والتأكد من إجراء التحديثات اليدوية متى ما كانت التحديثات والإصلاحات الآلية غير مدعومة.
٦	تفعيل وحماية السجلات المناسبة ودمجها مع نظام إدارة السجلات المركزي.
٧	تهيئة جميع برامج الإدارة وبرامج الحماية ونظام التشغيل على الأصول المعلوماتية والتقنية.
٨	الإشراف على صلاحيات الوصول وحسابات المستخدمين للأصول المعلوماتية والتقنية حسب السياسة الخاصة بها.
٩	مراعاة عزل الأصول المعلوماتية والتقنية والتقسيم المنطقي لأجزاء الشبكات بشكل آمن.
١٠	المشاركة في إدارة التهديدات والحوادث في أنظمة تقنية المعلومات في المراحل المعنية بها (مثل: مراحل الاحتواء (Containment)، والاستئصال (Eradication)، والتعافي أو الاستعادة Recovery).)

#	المسؤوليات
١١	المساعدة في تحديد وترتيب أولويات قدرات الأنظمة ووحدات الأعمال الأساسية اللازمة لاستعادة النظام المعني كليًا أو جزئيًا بعد وقوع حدث كارثي يتسبب في فشل متعلق بالأمن السيبراني.
١٢	المساعدة في تحديد المستويات الملائمة لتوافر المعلومات في الأنظمة، وذلك استنادًا 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
١	الإشراف على تنفيذ متطلبات الأمن السيبراني المتعلقة بالموارد البشرية في <اسم الجهة>.
٢	التأكد من إجراء المسح الأمني للعاملين في وظائف الأمن السيبراني والوظائف التقنية ذات الصلاحيات الهامة والحساسة بالتنسيق مع الجهات المعنية.
٣	تولي المسؤولية المتعلقة بدعم تطبيق سياسة الاستخدام المقبول للأصول وتطبيق العقوبات على المخالفين حسب الإجراءات المعتمدة لدى <اسم الجهة>.
٤	تحديث ومراجعة سياسة الأمن السيبراني المتعلقة بالموارد البشرية.
٥	حضور اجتماعات اللجنة الإشرافية للأمن السيبراني والمشاركة بها حسب الضرورة.
٦	المطالبة بالتمويل الكافي للموارد التدريبية المتعلقة بالأمن السيبراني، بما في ذلك الدورات الداخلية والدورات المتعلقة بالقطاع، والمدربين والمواد ذات الصلة.
٧	إجراء تقييمات الاحتياجات التعليمية وتحديد المتطلبات المتعلقة بالأمن السيبراني.
٨	التأكد من إعداد وتنفيذ أدوار ومسؤوليات وظيفية قياسية وفقًا للأدوار الوظيفية المحددة المتعلقة بالأمن السيبراني.
٩	تحديد المسارات المهنية للأمن السيبراني لإتاحة الفرصة للنمو المهني والترقيات في المجالات المهنية المتعلقة بالأمن السيبراني.

١٠	التنسيق مع <الإدارة المعنية بالأمن السيبراني> حول المسائل المتعلقة بالأمن السيبراني التي تؤثر على <الإدارة المعنية بالموارد البشرية>.
١١	المشاركة في مراجعة استراتيجية وسياسات الأمن السيبراني وتقديم المدخلات لها.
١٢	التعامل مع مخالفات عدم الالتزام بسياسات الأمن السيبراني وذلك بالتنسيق مع <الإدارة المعنية بالشؤون القانونية>.

موظفو <الإدارة المعنية بالموارد البشرية>

#	المسؤوليات
١	تنفيذ متطلبات الأمن السيبراني المتعلقة بالموارد البشرية في <اسم الجهة>.
٢	إجراء المسح الأمني للعاملين في وظائف الأمن السيبراني والوظائف التقنية ذات الصلاحيات الهامة والحساسة بالتنسيق مع الجهات المعنية.
٣	إجراء تقييم للوعي الأمني لجميع العاملين وتحديد نقاط الضعف المتعلقة بالأمن السيبراني والعمل على معالجتها.
٤	تنفيذ برنامج التوعية والتدريب بالأمن السيبراني بالتنسيق مع الإدارة المعنية بالتوعية والتدريب بالأمن السيبراني.
٥	إعداد وتنفيذ أوصاف وظيفية قياسية وفقًا للأدوار الوظيفية المحددة المتعلقة بالأمن السيبراني.
٦	المساعدة في تحديد المسارات المهنية للأمن السيبراني لإتاحة الفرصة للنمو المهني والترقيات في المجالات المهنية المتعلقة بالأمن السيبراني.
٧	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
١	الإشراف على المراجعة والتدقيق الدوري لبرامج ومتطلبات الأمن السيبراني وفقًا لمعايير التدقيق المقبولة عمومًا (GAAS)، والقوانين والتنظيمات ذات العلاقة.
٢	الإشراف على تدقيق الأمن السيبراني وفقًا لشروط سياسة تدقيق ومراجعة الأمن السيبراني.
٣	التأكد من المراجعة والتحديث الدوري لجميع الوثائق المتعلقة بالأمن السيبراني.
٤	التعاون مع إدارة الأمن السيبراني لحضور اجتماعات اللجنة الإشرافية للأمن السيبراني والمشاركة بها حسب الضرورة.
٥	التأكد من تحديث مخاطر الأمن السيبراني وإعادة تقييمها وفقًا لسياسة إدارة مخاطر الأمن السيبراني.
٦	التأكد من مواءمة قبول المخاطر مع سياسة إدارة مخاطر الأمن السيبراني.
٧	اقتراح خطّة معالجة لنتائج وملاحظات التدقيق.
٨	توثيق النتائج والملاحظات والإبلاغ عنها ومناقشتها مع الإدارة المعنية.
٩	تقديم نتائج وملاحظات التدقيق إلى اللجنة الإشرافية المعنية بالأمن السيبراني.
١٠	مناقشة الإجراءات التصحيحية مع مسؤولي نتائج التدقيق وتوثيقها.
١١	الإبلاغ عن أي ضوابط غير فعّالة متعلّقة بالأمن السيبراني.
١٢	الإبلاغ عن عدم الالتزام بمتطلبات الأمن السيبراني.
١٣	التنسيق مع فريق الأمن السيبراني حول المسائل المتعلقة بالأمن السيبراني التي تؤثر على الإدارة المعنية بالتدقيق الداخلي.
١٤	مراجعة استراتيجية وسياسات الأمن السيبراني وتقديم المدخلات لها.

موظفو <الإدارة المعنية بالتدقيق الداخلي>

#	المسؤوليات
١	المساعدة في مراجعة وتدقيق تنفيذ ضوابط الأمن السيبراني وفقًا لمعايير التدقيق المتعارف عليها والمقبولة عمومًا، والقوانين والتنظيمات ذات العلاقة.
٢	تنفيذ متطلبات الأمن السيبراني المتعلقة بالتدقيق الداخلي في <اسم الجهة>.
٣	المراجعة والتحديث الدوري لجميع الوثائق المتعلقة بالأمن السيبراني.
٤	إجراء مراجعات للتأكّد من تحديث مخاطر الأمن السيبراني وإعادة تقييمها وفقًا لسياسة إدارة مخاطر الأمن السيبراني.
٥	إجراء مراجعات للتأكد من مواءمة قبول المخاطر مع سياسة إدارة مخاطر الأمن السيبراني.
٦	إجراء مراجعات وإبلاغ رئيس التدقيق الداخلي بعدم الالتزام بمتطلبات الأمن السيبراني.
٧	تنفيذ عملية تدقيق الأمن السيبراني وفقًا لشروط سياسة تدقيق ومراجعة الأمن السيبراني.
٨	تحليل الضوابط الفعّالة للأمن السيبراني، وتقديم التوصيات لرئيس التدقيق الداخلي بشأنها.
٩	اقتراح الإجراءات التصحيحية على رئيس التدقيق الداخلي وفقًا لنتائج وملاحظات التدقيق.
١٠	المساعدة في اقتراح خطّة معالجة لنتائج وملاحظات التدقيق.
١١	المساعدة في التنسيق مع فريق الأمن السيبراني حول المسائل المتعلقة بالأمن السيبراني التي تؤثر على الإدارة المعنية بالتدقيق الداخلي.

<الإدارة المعنية بالشؤون القانونية>

#	المسؤوليات
١	حصر المتطلبات التنظيمية والتشريعية الوطنية ذات العلاقة بالأمن السيبراني، والاتفاقيات والالتزامات الدولية المعتمدة محليًا التي تتضمن متطلبات خاصة بالأمن السيبراني تنطبق على <اسم الجهة>.
٢	ترجمة ضوابط الأمن السيبراني وتنظيماته وسياساته ومعاييره وإجراءاته، وجعلها ملزمة قانونيًا.

#	المسؤوليات
٣	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>.
٤	الإشراف على تنفيذ متطلبات الأمن السيبراني المتعلقة بالشؤون القانونية في <اسم الجهة>.
٥	حضور اجتماعات اللجنة الإشرافية للأمن السيبراني والمشاركة بها حسب الضرورة.
٦	تقييم فعالية قوانين وتنظيمات الأمن السيبراني.
٧	مراجعة سياسة أمن الأطراف الخارجية المعتمدة في <اسم الجهة> وفقًا للمتطلّبات القانونية ذات العلاقة.
٨	العمل مع <الإدارة المعنية بالأمن السيبراني> حول المسائل المتعلقة بالأمن السيبراني التي تؤثر على الإدارة المعنية بالشؤون القانونية.
٩	تقديم الدعم لحوادث الأمن السيبراني عند الحاجة.

موظفو <الإدارة المعنية بالشؤون القانونية>

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

جميع العاملين في <اسم الجهة>

#	المسؤوليات
١	التعامل مع البيانات والمعلومات حسب مستوى تصنيفها.

٢	تلافي انتهاك حقوق أي شخص أو شركة محمية بحقوق النشر أو براءة الاختراع أو أي ملكية فكرية أخرى أو قوانين أو لوائح مماثلة.
٣	الالتزام بسياسات وإجراءات الأمن السيبراني.
٤	الالتزام بمتطلبات الأمن السيبراني المتعلقة بحماية أجهزة المستخدمين.
٥	الالتزام بمتطلبات الأمن السيبراني المتعلقة باستخدام الإنترنت والبرمجيات.
٦	الالتزام بمتطلبات الأمن السيبراني المتعلقة بالبريد الإلكتروني.
٧	الالتزام بالمتطلبات المتعلقة بنظم وتقنيات حماية الأمن السيبراني.
٨	استخدام جميع الأصول المعلوماتية والتقنية الخاصة بـ<اسم الجهة> لأغراض العمل فقط وحسب سياسة الاستخدام المقبول للأصول المعتمدة في <اسم الجهة>.
٩	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>.
١٠	الإبلاغ عن حوادث الأمن السيبراني.
١١	الالتزام بسياسة الاستخدام المقبول.

جدول فصل مهام إدارة وتشغيل الأنظمة والأدوات المتعلقة بالأمن السيبراني

جوانب الحوكمة والمخاطر والالتزام لجميع الأنظمة والأدوات المتعلقة بالأمن السيبراني تعتبر مسؤولية <الإدارة المعنية بالأمن السيبراني>، أما فيما يتعلق بإدارة وتشغيل الأنظمة والأدوات فالمسؤولية تختلف بحسب النظام أو الأداة المستخدمة حيث تم توضيح مسؤولية إدارة وتشغيل الأنظمة والأدوات المتعلقة بالأمن السيبراني في الجدول أدناه:

الأنظمة والأدوات المتعلقة بالأمن السيبراني	مسؤولية إدارة وتشغيل الأنظمة والأدوات	
	<الإدارة المعنية بالأمن السيبراني>	<الإدارة المعنية بتقنية المعلومات>
أنظمة وأدوات إدارة هويات الدخول والصلاحيات		✓
أنظمة وأدوات إدارة الصلاحيات الهامة والحساسة		✓
أنظمة وأدوات إدارة سجلات الأحداث ومراقبة الأمن السيبراني	✓	
أنظمة وأدوات أمن الشبكات (مثل جدران الحماية)		✓
أدوات اختبار الاختراق	✓	
أدوات فحص واكتشاف وتقييم الثغرات التقنية	✓	
أدوات المعلومات الاستباقية	✓	
أنظمة وأدوات إدارة الحوكمة والمخاطر والالتزام	✓	
أدوات التحليل الجنائي الرقمي	✓	
أدوات الاستجابة لحوادث الأمن السيبراني	✓	
أنظمة وأدوات الحماية من الحماية من الفيروسات والبرامج والنشطة المشبوهة والبرمجيات		✓
أنظمة وأدوات النسخ الاحتياطية		✓
أنظمة وأدوات تصنيف البيانات		✓
أنظمة وأدوات منع فقدان البيانات		✓
أنظمة وأدوات التشفير		✓
أنظمة وأدوات إدارة الأجهزة المحمولة		✓

الأنظمة والأدوات المتعلقة بالأمن السيبراني	مسؤولية إدارة وتشغيل الأنظمة والأدوات	
	<الإدارة المعنية بالأمن السيبراني>	<الإدارة المعنية بتقنية المعلومات>
أنظمة وأدوات إدارة الأصول		✓

الأدوار والمسؤوليات

١- **مالك الوثيقة:** <رئيس الإدارة المعنية بالأمن السيبراني>.
٢- **مراجعة الوثيقة وتحديثها:** <الإدارة المعنية بالأمن السيبراني>.
٣- **تنفيذ الوثيقة وتطبيقها:** < الإدارة المعنية بالأمن السيبراني> و<الإدارة المعنية بالموارد البشرية>.
٤- **مراجعة الالتزام بالوثيقة:** <الإدارة المعنية بالأمن السيبراني>.

التحديث والمراجعة

يجب على <الإدارة المعنية بالأمن السيبراني> مراجعة الوثيقة سنويًا على الأقل أو في حال حدوث تغييرات في السياسات أو الإجراءات التنظيمية في <اسم الجهة> أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

الالتزام بالوثيقة

١- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> التأكد من التزام <اسم الجهة> بهذه الوثيقة دوريًا.
٢- يجب على كافة العاملين في <اسم الجهة> الالتزام بهذه الوثيقة.

جدول المراجع

اللائحة ذات الصلة	المرجع في ضوابط التنظيم	رقم الضابط
الضوابط الأساسية للأمن السيبراني(ECC)	١-٤-١	١-٤
	١-٤-٢	١-٤