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

أدخل شعار الجهة بالضغط على الصورة الموضحة.

نموذج الهيكل التنظيمي للأمن السيبراني

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

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

اختر التصنيف

التاريخ: اضغط هنا لإضافة نص

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

اعتماد الوثيقة

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

نسخ الوثيقة

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

جدول المراجعة

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

قائمة المحتويات

الأهداف

تهدف هذه الوثيقة إلى تحديد وتوثيق الهيكل التنظيمي للحوكمة والأدوار والمسؤوليات الخاصة بالأمن السيبراني ل<الإدارة المعنية بالأمن السيبراني> في <اسم الجهة> والمستقلة عن <الإدارة المعنية بتقنية المعلومات> وفقاً للأمر السامي الكريم رقم ٣٧١٤٠ بتاريخ ١٤٣٨/٨/١٤هـ ووفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة، حيث أن إنشاء هذه الإدارة واستقلالها مطلب تشريعي من الضوابط الصادرة من الهيئة الوطنية للأمن السيبراني والمتطلبات التنظيمية والتشريعية ذات العلاقة.

تم تطوير هذه الوثيقة بناءً على أفضل الممارسات والمعايير اللازمة لتوفير الدعم ل<الإدارة المعنية بالأمن السيبراني> لتمكينها من تنفيذ المهام الموكلة إليها بالشكل المطلوب. وتُعد <الإدارة المعنية بالأمن السيبراني> أحد الروافد الأساسية في <اسم الجهة> وهي المعنية بحماية الأصول المعلوماتية والتقنية من المخاطر السيبرانية.

القواعد الإرشادية

١- التأكد من أن <الإدارة المعنية بالأمن السيبراني> مستقلة عن <الإدارة المعنية بتقنية المعلومات>.
٢- التأكد من أن <الإدارة المعنية بالأمن السيبراني> مرتبطة برئيس الجهة أو من ينيبه في <اسم الجهة> بحيث يمكنه التأثير على القرارات الرئيسية المتعلقة بالأمن السيبراني في <اسم الجهة>.
٣- التأكد من أن ارتباط <الإدارة المعنية بالأمن السيبراني> مختلف عن ارتباط <الإدارة المعنية بتقنية المعلومات> أو <الإدارة المعنية بالتحول الرقمي> تنفيذًا للأمر السامي الكريم رقم ٣٧١٤٠ بتاريخ ١٤٣٨/٨/١٤هـ، وهو مطلب تشريعي في الضابط رقم ١-٢-١ من الضوابط الأساسية للأمن السيبراني (ECC-١:٢٠١٨).
٤- تجنب تعارض المصالح، ومن أمثلة تعارض المصالح ما يلي:
٤-١ إدارة صلاحية الأنظمة التقنية والمعلوماتية (أو الأنظمة التشغيلية) وإدارة عملياتها في الوقت ذاته.
٤-٢ تطبيق متطلبات الأمن السيبراني والتأكد من الالتزام بها في الوقت ذاته.
٤-٣ تعارض مصالح فريق مراقبة الأمن السيبراني مع فريق تشغيل عمليات الأمن السيبراني.
٤-٤ تعارض مصالح فريق الاختبارات الأمنية مع فريق تطوير التطبيقات.
٥- التأكد من وجود الأدوار التالية كحد أدنى في هيكلية الأمن السيبراني:
٥-١ حوكمة الأمن السيبراني.
٥-٢ إدارة الالتزام بالأمن السيبراني.
٥-٣ إدارة مخاطر الأمن السيبراني.
٥-٤ إدارة استراتيجية الأمن السيبراني.
٥-٥ صمود الأمن السيبراني.
٥-٦ التوعية والتدريب بالأمن السيبراني.
٥-٧ عمليات الأمن السيبراني (مراقبة الأمن السيبراني والاستجابة للحوادث).
٥-٨ حماية البيانات والمعلومات.
٥-٩ الأمن السيبراني للأنظمة التشغيلية OT/ICS (إن وجد).
٦- قد تضاف الأدوار التالية إلى هيكلية الأمن السيبراني:
٦-١ معمارية الأمن السيبراني.

٦-٢ إدارة هويات الدخول والصلاحيات.
٦-٣ إدارة بنية الأمن السيبراني التحتية.
٦-٤ الأمن المادي.

حوكمة الأمن السيبراني

عناصر الهيكل التنظيمي لـ<اسم الجهة>

#	العنصر	الوصف
١	صاحب الصلاحية	هو رئيس الجهة أو من ينيبه.
٢	اللجنة الإشرافية للأمن السيبراني	اللجنة الإشرافية للأمن السيبراني هي مجلس حوكمة رفيع المستوى، وتتمثّل مسؤوليتها الأساسية في ضمان التزام تطبيق برامج وتشريعات الأمن السيبراني داخل <اسم الجهة> ودعمها ومتابعتها.
٣	إدارة الأمن السيبراني	<الإدارة المعنية بالأمن السيبراني> هي المعنية بحماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات وما تقدمه من خدمات وما تحتويه من بيانات من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع. ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك.
٤	تقنية المعلومات	<الإدارة المعنية بتقنية المعلومات> هي الإدارة المعنية بتشغيل البنية التحتية لتقنية المعلومات والشبكات، وتطوير البرمجيات والخدمات التقنية، وغير ذلك من أعمال.
٥	الموارد البشرية	<الإدارة المعنية بالموارد البشرية> هي الإدارة المعنية بشؤون العاملين داخل <اسم الجهة>.
٦	الشؤون القانونية	<الإدارة المعنية بالشؤون القانونية> هي الإدارة المعنية بصياغة العقود والاتفاقيات وحفظ حقوق <اسم الجهة> القانونية.
٧	المشتريات	<الإدارة المعنية بشؤون المشتريات> هي الإدارة المعنية بالتعاقد مع الموردين وعمليات الشراء وكذلك عقود الأطراف الخارجية في <اسم الجهة>.
٨	الشؤون المالية	<الإدارة المعنية بالشؤون المالية> هي الإدارة المعنية بإعداد الميزانية العامة لـ<اسم الجهة>.

#	العنصر	الوصف
٩	مكتب إدارة البيانات	<الإدارة المعنية بإدارة البيانات> هي الإدارة المعنية بإدارة البيانات والخصوصية في <اسم الجهة>.
١٠	التدقيق والمراجعة الداخلية	<الإدارة المعنية بالمراجعة الداخلية> هي الإدارة المعنية بتدقيق ومراجعة تطبيق <اسم الجهة> للسياسات والإجراءات وكذلك المتطلبات التنظيمية والتشريعية ذات العلاقة.
١١	إدارة استمرارية الأعمال	<الإدارة المعنية باستمرارية الأعمال> هي الإدارة المعنية بجميع المسائل المتعلّقة باستمرارية الأعمال في <اسم الجهة>. والتي تشمل إدارة الأزمات والتعافي من الكوارث.
١٢	تقنية التشغيل	<الإدارة المعنية بتقنية التشغيل> (Operational Technology) هي الإدارة المعنية بجميع المسائل المتعلّقة بالتقنية التشغيلية في <اسم الجهة>.
١٣	مكتب إدارة المشاريع	<مكتب إدارة المشاريع> هو المعني بجميع المسائل المتعلّقة بإدارة المشاريع في <اسم الجهة>، بما في ذلك مكاتب تحقيق الرؤية ٢٠٣٠ (إن وجدت).
١٤	وحدات الأعمال	تشمل جميع وحدات الأعمال والإدارات الأخرى في <اسم الجهة>.

هيكلية الأمن السيبراني

تم توزيع المهام والأدوار في <الإدارة المعنية بالأمن السيبراني> بناءً على الوظائف التشغيلية لكل دور، وذلك لتقوم <الإدارة المعنية بالأمن السيبراني> بعملها بالشكل المطلوب وبكفاءة عالية مع الأخذ بعين الاعتبار مبدأ فصل المهام (Segregation of Duties) وتلافي تعارض المصالح (Conflict of Interest) وتم توزيعها كالتالي <يمكن اختيار أحد الخيارات أدناه>:

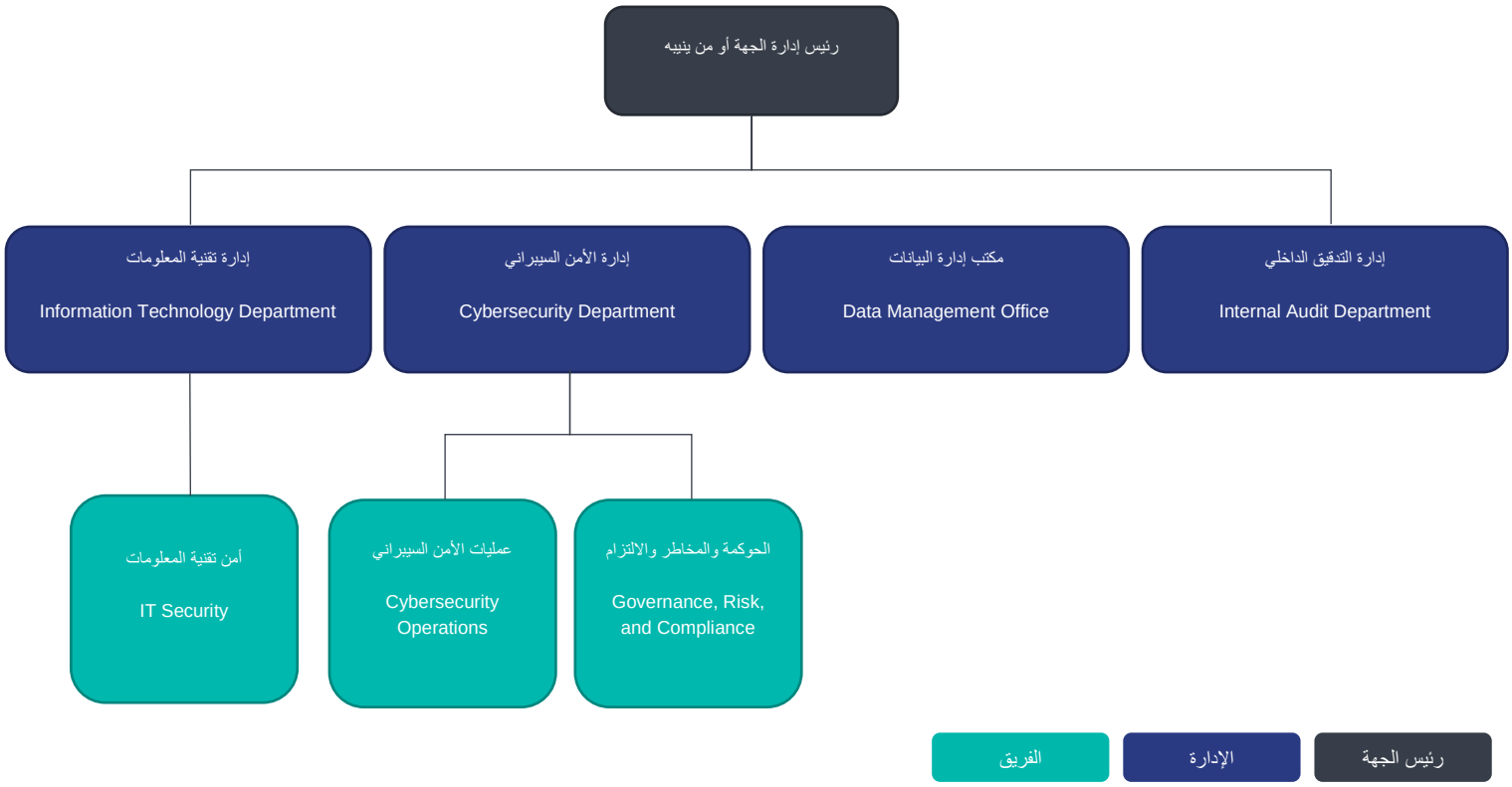
الهيكل التنظيمي <للإدارة المعنية بالأمن السيبراني>

الهياكل التنظيمية التالية المقترحة تعتبر اختيارية، يمكن اختيار الهيكل بناءً على ما يتناسب مع طبيعة أعمال ومهام الجهة وحجمها.

١- الخيار الأول

١-١ يتوافق هذا الهيكل التنظيمي للأمن السيبراني مع التنظيميات الوطنية ذات العلاقة بالأمن السيبراني ومنها على سبيل المثال لا الحصر: ECC-١:٢٠١٨ .

١-٢ يخلو هذا الهيكل التنظيمي للأمن السيبراني من التعقيد ويعتبر أسهل من ناحية الفهم والتنفيذ.



إدارة الأمن السيبراني		
#	الأدوار	الوصف
١	مستشار الأمن السيبراني	تقديم الرأي والمشورة لقيادة الجهة وقادة وفرق الأمن السيبراني في مواضيع الأمن السيبراني.

الحوكمة والمخاطر والالتزام		
#	الأدوار	الوصف
١	مصمم معمارية الأمن السيبراني	تصميم نُظم وشبكات الأمن السيبراني، والإشراف على إعداداتها وتطويرها وتنفيذها.

٢	أخصائي الحوسبة السحابية الآمنة	تصميم نظم الحوسبة السحابية الآمنة وتنفيذها وتشغيلها، مع تطوير سياسات السحابة الآمنة.
٣	مقيم البرمجيات الآمنة	تقييم أمن تطبيقات الحاسب وبرمجياته وشفراته أو برامجه، مع تقديم نتائج قابلة للتطبيق.
٤	باحث الأمن السيبراني	إجراء الأبحاث العلمية في مجال الأمن السيبراني.
٥	أخصائي مخاطر الأمن السيبراني	تحديد مخاطر الأمن السيبراني للمنظمة وتقييمها وإدارتها لحماية أصولها المعلوماتية والتقنية وفقاً لسياسات وإجراءات الجهة، وكذلك القوانين والأنظمة ذات العلاقة.
٦	أخصائي الالتزام في الأمن السيبراني	ضمان التزام برنامج الأمن السيبراني للمنظمة بالمتطلبات والسياسات والمعايير الواجب تطبيقها.
٧	أخصائي سياسات الأمن السيبراني	تطوير سياسات الأمن السيبراني وتحديثها، لدعم متطلبات الأمن السيبراني بالجهة ومواءمتها.
٨	مُقيّم ضوابط الأمن السيبراني	تحليل ضوابط الأمن السيبراني وتقييم فاعليتها.
٩	أخصائي الأمن السيبراني	تقديم الدعم العام للأمن السيبراني، والمساعدة في مهام الأمن السيبراني.
١٠	مصمم معمارية الأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية	تصميم نُظم وشبكات الأمن السيبراني في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية والإشراف على إعداداتها وتطويرها وتنفيذها.
١١	أخصائي مخاطر الأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية	تحديد مخاطر الأمن السيبراني في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية وتقييمها وإدارتها، مع تقييم وتحليل فاعلية ضوابط الأمن السيبراني القائمة، وتقديم الملاحظات والتوصيات بناء على تلك التقييمات.
١٢	أخصائي قانون الأمن السيبراني	تقديم الخدمات القانونية بشأن الموضوعات ذات الصلة بالقوانين والأنظمة السيبرانية.

#	الأدوار	الوصف
١	محلل دفاع الأمن السيبراني	استخدام البيانات التي تم استخلاصها من مجموعة أدوات الدفاع السيبراني لتحليل الأحداث الواقعة داخل الجهة بهدف الكشف عن التهديدات والتعامل معها.
٢	أخصائي تقييم الثغرات	تقييم ثغرات النُظم والشبكات، وتحديد مواطن انحرافها عن الإعدادات المقبولة أو السياسات المعمول بها، وقياس فاعلية البنية الدفاعية متعددة الطبقات ضد الثغرات المعروفة.
٣	أخصائي اختبار الاختراقات	أداء محاولات اختراق مصرح لها لأنظمة الحاسبات أو الشبكات أو المنشآت المادية باستخدام أساليب تهديد واقعية لتقييم حالتها الأمنية وكشف الثغرات المحتملة.
٤	أخصائي استجابة للحوادث السيبرانية	مباشرة الحوادث المتعلقة بالأمن السيبراني وتحليلها والاستجابة لها.
٥	أخصائي التحليل الجنائي الرقمي	جمع الأدلة الرقمية وتحليلها، والتحقيق في حوادث الأمن السيبراني لاستخلاص معلومات مفيدة لمعالجة ثغرات النُظم والشبكات.
٦	أخصائي تحقيقات الجرائم السيبرانية	تعريف الأدلة وجمعها وفحصها والحفاظ عليها، باستخدام أساليب تحرٍ واستقصاء موثقة ومقننة.
٧	أخصائي الهندسة العكسية للبرمجيات الضارة	تحليل البرمجيات الضارة (عن طريق تفكيكها وإعادتها إلى صيغة برمجية مفهومة)، وفهم طريقة عملها وتأثيرها وغرضها، وتقديم توصيات للوقاية منها والاستجابة للحوادث الناتجة عنها.
٨	محلل معلومات التهديدات السيبرانية	جمع معلومات عن التهديدات السيبرانية من مصادر مختلفة وتحليلها لتكوين فهم وإدراك عميقين للتهديدات السيبرانية، وخطط المخترقين، والأساليب والخطط المتبعة، لاستنباط وتوثيق مؤشرات من شأنها مساعدة المنظمات في الكشف عن الحوادث السيبرانية والتنبؤ بها، وحماية النُظم والشبكات من التهديدات السيبرانية.
٩	أخصائي اكتشاف التهديدات السيبرانية	البحث الاستباقي عن التهديدات غير المكتشفة في الشبكات والنُظم، وتحديد مؤشرات الاختراق، وتقديم التوصيات للتعامل معها.

١٠	محلل دفاع الأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية	استخدام البيانات، التي تم جمعها من مجموعة متنوعة من أدوات الأمن السيبراني لتحليل الأحداق الواقعة في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية بهدف الكشف عن تهديدات الأمن السيبراني والتعامل معها.

أمن تقنية المعلومات		
#	الأدوار	الوصف
١	أخصائي تطوير أمن النظم	تصميم أمن نُظم المعلومات وتطويره واختباره وتقييمه في كافة مراحل تطوير تلك النُظم.
٢	مطور الأمن السيبراني	تطوير برمجيات الأمن السيبراني وتطبيقاته ونُظمه ومنتجاته.
٣	أخصائي البنية التحتية للأمن السيبراني	فحص وتنصيب وصيانة الأجهزة والبرمجيات المستخدمة للدفاع وحماية الأنظمة والشبكات من التهديدات السيبرانية وتشغيلها والإشراف عليها.
٤	أخصائي التشفير	تطوير أنظمة التشفير وخوارزمياته.
٥	أخصائي إدارة الهوية والوصول	إدارة هوية الأفراد والكيانات، وصلاحيات وصولهم إلى الموارد من خلال تطبيق أنظمة، وعمليات التعريف، والتوثيق، والتصريح.
٦	محلل أمن النظم	تطوير أمن النُظم واختباره وصيانته، وتحليل أمن العمليات والأنظمة المدمجة.

مكتب إدارة البيانات		
#	الأدوار	الوصف
١	أخصائي علم البيانات للأمن السيبراني	استخدام نماذج رياضية ومنهجيات وعمليات علمية لتصميم وتنفيذ خوارزميات وأنظمة لاستخلاص استنتاجات ومعارف الأمن السيبراني من مصادر متعددة لمجموعة بيانات واسعة النطاق.

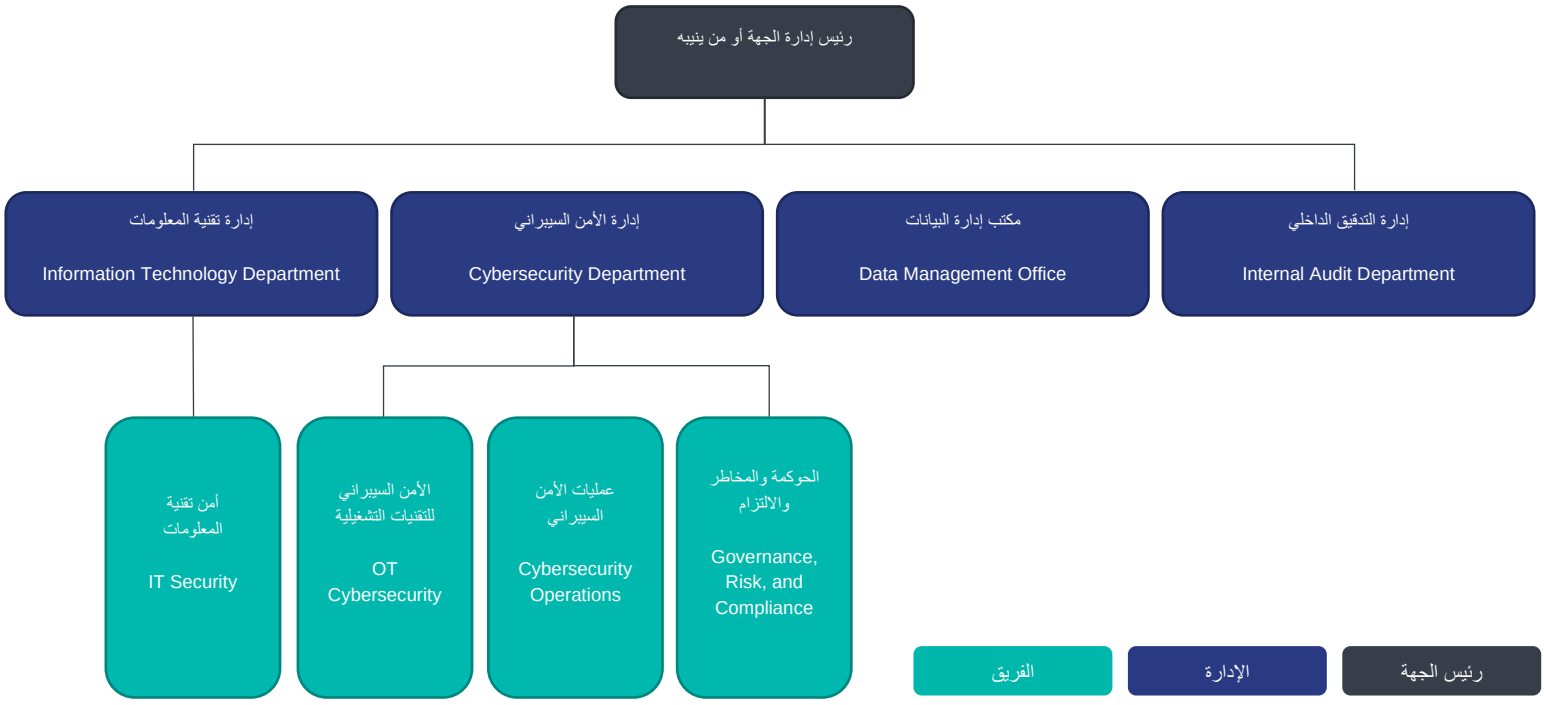
٢	أخصائي الذكاء الاصطناعي للأمن السيبراني	استخدام نماذج الذكاء الاصطناعي وتقنياته (شاملاً أساليب التعلم الآلي) لتصميم وتنفيذ خوارزميات وأنظمة لأتمتة وتحسين كفاءة وفعالية مهام الأمن السيبراني.
٣	أخصائي الخصوصية وحماية البيانات	دراسة هيكلة البيانات الشخصية وقوانين وأنظمة الخصوصية المعمول بها، مع تحليل مخاطر الخصوصية، وتطوير برنامج الجهة للمواءمة مع ضوابط الخصوصية وحماية البيانات والسياسات الداخلية، والإشراف على تنفيذها، مع دعم استجابة الجهة لحوادث الخصوصية أو حماية البيانات.

مكتب التدقيق الداخلي		
#	الأدوار	الوصف
١	مدقق الأمن السيبراني	تصميم عمليات التدقيق للأمن السيبراني وتنفيذها وإدارتها بهدف تقييم مدى التزام الجهة بالمتطلبات والسياسات والمعايير والضوابط المعمول بها، وإعداد تقارير التدقيق وتقديمها للأطراف ذات الصلاحية.

٢- الخيار الثاني

٢-١ يُركّز هذا الهيكل التنظيمي للأمن السيبراني بشكل خاص على الخصوصية والشؤون القانونية.

٢-٢ يُتيح هذا الهيكل التنظيمي حماية سريّة وسلامة وتوافر أصول <اسم الجهة> المتعلّقة بأجهزة وأنظمة التحكم الصناعي (OT/ICS) ضد الهجمات السيبرانية.



الحوكمة والمخاطر والالتزام		
#	الأدوار	الوصف
١ ١	مستشار الأمن السيبراني مصمم معمارية الأمن السيبراني	تقديم الرأي والمشورة لقيادة الجهة ووحدة وفرق الأمن السيبراني في مواضيع الأمن السيبراني. تصميم نُظم وشبكات الأمن السيبراني، والإشراف على إعداداتها وتطويرها وتنفيذها.
٢	أخصائي الحوسبة السحابية الآمنة	تصميم نظم الحوسبة السحابية الآمنة وتنفيذها وتشغيلها، مع تطوير سياسات السحابة الآمنة.
٣	مقيم البرمجيات الآمنة	تقييم أمن تطبيقات الحاسب وبرمجياته وشفراته أو برامجه، مع تقديم نتائج قابلة للتطبيق.
٤	باحث الأمن السيبراني	إجراء الأبحاث العلمية في مجال الأمن السيبراني.
٥	أخصائي مخاطر الأمن السيبراني	تحديد مخاطر الأمن السيبراني للمنظمة وتقييمها وإدارتها لحماية أصولها المعلوماتية والتقنية وفقاً لسياسات وإجراءات الجهة، وكذلك القوانين والأنظمة ذات العلاقة.
٦	أخصائي الالتزام في الأمن السيبراني	ضمان التزام برنامج الأمن السيبراني للمنظمة بالمتطلبات والسياسات والمعايير المعمول بها.
٧	أخصائي سياسات الأمن السيبراني	تطوير سياسات الأمن السيبراني وتحديثها، لدعم متطلبات الأمن السيبراني بالجهة ومواءمتها.
٨	مُقيّم ضوابط الأمن السيبراني	تحليل ضوابط الأمن السيبراني وتقييم فاعليتها.
٩	أخصائي الأمن السيبراني	تقديم الدعم العام للأمن السيبراني، والمساعدة في مهام الأمن السيبراني.
١٠	أخصائي قانون الأمن السيبراني	تقديم الخدمات القانونية بشأن الموضوعات ذات الصلة بالقوانين والأنظمة السيبرانية.

عمليات الأمن السيبراني		
#	الأدوار	الوصف
١	محلل دفاع الأمن السيبراني	استخدام البيانات التي تم استخلاصها من مجموعة أدوات الدفاع السيبراني لتحليل الأحداث الواقعة داخل الجهة بهدف الكشف عن التهديدات والتعامل معها .
٢	أخصائي تقييم الثغرات	تقييم ثغرات النُظم والشبكات، وتحديد مواطن انحرافها عن الإعدادات المقبولة أو السياسات المعمول بها، وقياس فاعلية البنية الدفاعية متعددة الطبقات ضد الثغرات المعروفة.
٣	أخصائي اختبار الاختراقات	أداء محاولات اختراق مصرح لها لأنظمة الحاسبات أو الشبكات أو المنشآت المادية باستخدام أساليب تهديد واقعية لتقييم حالتها الأمنية وكشف الثغرات المحتملة.
٤	أخصائي استجابة للحوادث السيبرانية	مباشرة الحوادث المتعلقة بالأمن السيبراني وتحليلها والاستجابة لها.
٥	أخصائي التحليل الجنائي الرقمي	جمع الأدلة الرقمية وتحليلها، والتحقيق في حوادث الأمن السيبراني لاستخلاص معلومات مفيدة لمعالجة ثغرات النُظم والشبكات.
٦	أخصائي تحقيقات الجرائم السيبرانية	تعريف الأدلة وجمعها وفحصها والحفاظ عليها، باستخدام أساليب تحرٍ واستقصاء موثقة ومقننة.
٧	أخصائي الهندسة العكسية للبرمجيات الضارة	تحليل البرمجيات الضارة (عن طريق تفكيكها وإعادتها إلى صيغة برمجية مفهومة)، وفهم طريقة عملها وتأثيرها وغرضها، وتقديم توصيات للوقاية منها والاستجابة للحوادث الناتجة عنها.
٨	محلل معلومات التهديدات السيبرانية	جمع معلومات عن التهديدات السيبرانية من مصادر مختلفة وتحليلها لتكوين فهم وإدراك عميقين للتهديدات السيبرانية، وخطط المخترقين، والأساليب والخطط المتبعة، لاستنباط وتوثيق مؤشرات من شأنها مساعدة المنظمات في الكشف عن

		الحوادث السيبرانية والتنبؤ بها، وحماية النُظم والشبكات من التهديدات السيبرانية.
٩	أخصائي اكتشاف التهديدات السيبرانية	البحث الاستباقي عن التهديدات غير المكتشفة في الشبكات والنُظم، وتحديد مؤشرات الاختراق، وتقديم التوصيات للتعامل معها.

الأمن السيبراني للتقنيات التشغيلية		
#	الأدوار	الوصف
١	مصمم معمارية الأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية	تصميم نُظم وشبكات الأمن السيبراني في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية والإشراف على إعداداتها وتطويرها وتنفيذها.
٢	أخصائي مخاطر الأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية	تحديد مخاطر الأمن السيبراني في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية وتقييمها وإدارتها، مع تقييم وتحليل فاعلية ضوابط الأمن السيبراني القائمة، وتقديم الملاحظات والتوصيات بناء على تلك التقييمات.
٣	محلل دفاع الأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية	استخدام البيانات، التي تم جمعها من مجموعة متنوعة من أدوات الأمن السيبراني لتحليل الأحداق الواقعة في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية بهدف الكشف عن تهديدات الأمن السيبراني والتعامل معها.
٤	أخصائي البنية التحتية للأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية	فحص وتنصيب وصيانة الأجهزة والبرمجيات المستخدمة للدفاع وحماية الأنظمة والشبكات من التهديدات السيبرانية في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية وتشغيلها والإشراف عليها.
٥	أخصائي استجابة للحوادث السيبرانية لأنظمة التحكم الصناعي والتقنيات التشغيلية	مباشرة حوادث الأمن السيبراني وتحليلها والاستجابة لها في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية.

أمن تقنية المعلومات		
#	الأدوار	الوصف
١	أخصائي تطوير أمن النظم	تصميم أمن نُظم المعلومات وتطويره واختباره وتقييمه في كافة مراحل تطوير تلك النُظم.
٢	مطور الأمن السيبراني	تطوير برمجيات الأمن السيبراني وتطبيقاته ونُظمه ومنتجاته.
٣	أخصائي البنية التحتية للأمن السيبراني	فحص وتنصيب وصيانة الأجهزة والبرمجيات المستخدمة للدفاع وحماية الأنظمة والشبكات من التهديدات السيبرانية وتشغيلها والإشراف عليها.
٤	أخصائي التشفير	تطوير أنظمة التشفير وخوارزمياته.
٥	أخصائي إدارة الهوية والوصول	إدارة هوية الأفراد والكيانات، وصلاحيات وصولهم إلى الموارد من خلال تطبيق أنظمة، وعمليات التعريف، والتوثيق، والتصريح.
٦	محلل أمن النظم	تطوير أمن النُظم واختباره وصيانته، وتحليل أمن العمليات والأنظمة المدمجة.

مكتب إدارة البيانات		
#	الأدوار	الوصف
١	أخصائي علم البيانات للأمن السيبراني	استخدام نماذج رياضية ومنهجيات وعمليات علمية لتصميم وتنفيذ خوارزميات وأنظمة لاستخلاص استنتاجات ومعارف الأمن السيبراني من مصادر متعددة لمجموعة بيانات واسعة النطاق.
٢	أخصائي الذكاء الاصطناعي للأمن السيبراني	استخدام نماذج الذكاء الاصطناعي وتقنياته (شاملاً أساليب التعلم الآلي) لتصميم وتنفيذ خوارزميات وأنظمة لأتمتة وتحسين كفاءة وفعالية مهام الأمن السيبراني.
٣	أخصائي الخصوصية وحماية البيانات	دراسة هيكلة البيانات الشخصية وقوانين وأنظمة الخصوصية المعمول بها، مع تحليل مخاطر الخصوصية، وتطوير برنامج الجهة للمواءمة مع ضوابط الخصوصية وحماية البيانات والسياسات

		الداخلية، والإشراف على تنفيذها، مع دعم استجابة الجهة لحوادث الخصوصية أو حماية البيانات.

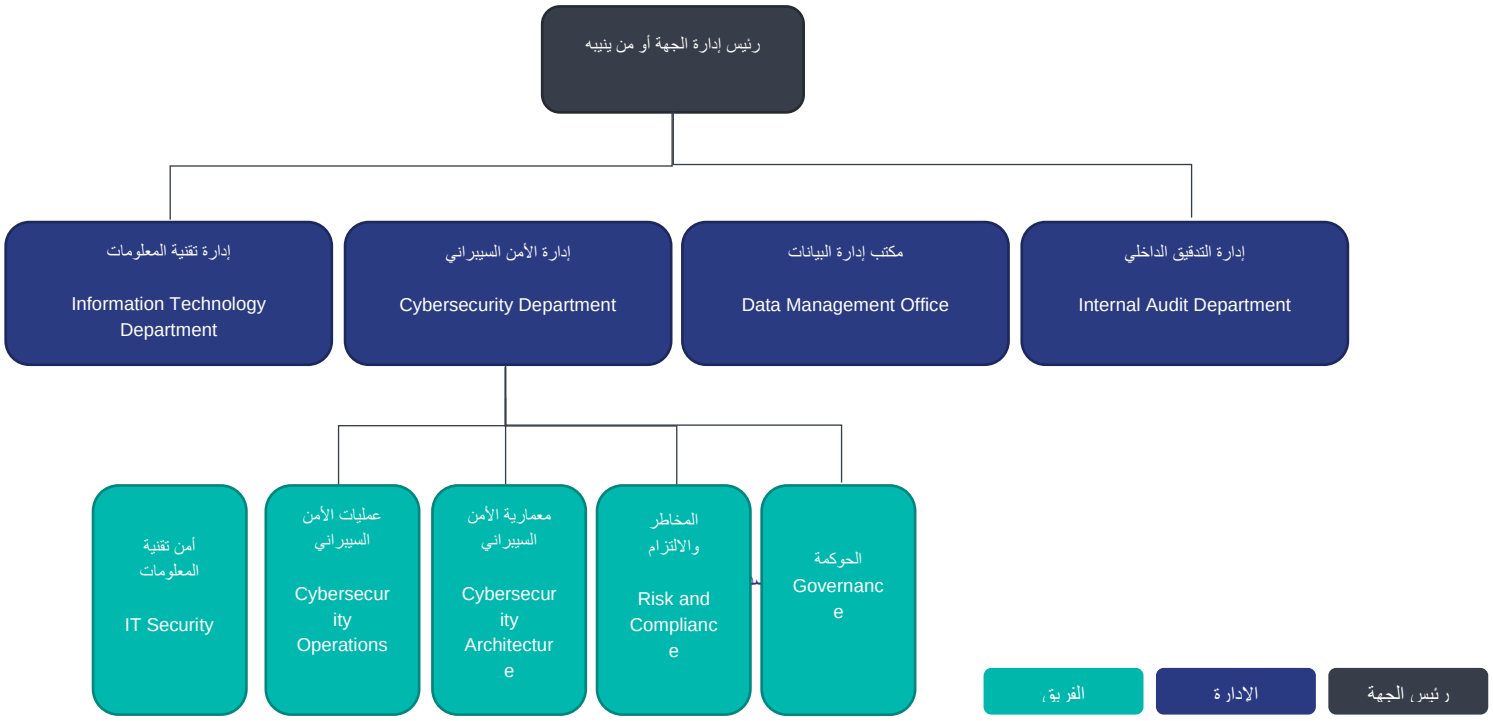
مكتب التدقيق الداخلي		
#	الأدوار	الوصف
١	مدقق الأمن السيبراني	تصميم عمليات التدقيق للأمن السيبراني وتنفيذها وإدارتها بهدف تقييم مدى التزام الجهة بالمتطلبات والسياسات والمعايير والضوابط المعمول بها، وإعداد تقارير التدقيق وتقديمها للأطراف ذات الصلاحية.

٣- الخيار الثالث

٣-١ يشمل هذا الخيار الإشراف على الميزانية، وتحمل مسؤولية التقنية الأمنية والقوة العاملة المعنية بتشغيل وإدارة هذه التقنية.

٣-٢ يُتيح الهيكل التنظيمي للأمن السيبراني استخدام تقنيات متطوّرة تُشجّع الابتكار السريع واعتماد الضوابط الأمنية الجديدة.

٣-٣ يُوفّر هذا الهيكل التنظيمي للأمن السيبراني مركز عمليات تشغيلي للأمن السيبراني، ويحظى فيه مدير مركز عمليات الأمن السيبراني على عدد أكبر من الموظفين والصلاحيات والسلطات.



إدارة الأمن السيبراني		
#	الأدوار	الوصف
١	مستشار الأمن السيبراني	تقديم الرأي والمشورة لقيادة الجهة وقادة وفرق الأمن السيبراني في مواضيع الأمن السيبراني.

الحوكمة		
#	الأدوار	الوصف
١	باحث الأمن السيبراني	إجراء الأبحاث العلمية في مجال الأمن السيبراني.
٢	أخصائي سياسات الأمن السيبراني	تطوير سياسات الأمن السيبراني وتحديثها، لدعم متطلبات الأمن السيبراني بالجهة ومواءمتها.
٣	أخصائي الأمن السيبراني	تقديم الدعم العام للأمن السيبراني، والمساعدة في مهام الأمن السيبراني.

المخاطر والالتزام		
#	الأدوار	الوصف
١	مقيم البرمجيات الآمنة	تقييم أمن تطبيقات الحاسب وبرمجياته وشفراته أو برامجه، مع تقديم نتائج قابلة للتطبيق.
٢	أخصائي مخاطر الأمن السيبراني	تحديد مخاطر الأمن السيبراني للمنظمة وتقييمها وإدارتها لحماية أصولها المعلوماتية والتقنية وفقاً لسياسات وإجراءات الجهة، وكذلك القوانين والأنظمة ذات العلاقة.
٣	أخصائي الالتزام في الأمن السيبراني	ضمان التزام برنامج الأمن السيبراني للمنظمة بالمتطلبات والسياسات والمعايير المعمول بها.

المخاطر والالتزام		
#	الأدوار	الوصف
٤	مقيم ضوابط الأمن السيبراني	تحليل ضوابط الأمن السيبراني وتقييم فاعليتها.
٥	أخصائي مخاطر الأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية	تحديد مخاطر الأمن السيبراني في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية وتقييمها وادارتها، مع تقييم وتحليل فاعلية ضوابط الأمن السيبراني القائمة، وتقديم الملاحظات والتوصيات بناء على تلك التقييمات.
٦	أخصائي قانون الأمن السيبراني	تقديم الخدمات القانونية بشأن الموضوعات ذات الصلة بالقوانين والأنظمة السيبرانية.

معمارية الأمن السيبراني		
#	الأدوار	الوصف
١	مصمم معمارية الأمن السيبراني	تصميم نُظم وشبكات الأمن السيبراني، والإشراف على إعداداتها وتطويرها وتنفيذها.
٢	أخصائي الحوسبة السحابية الآمنة	تصميم نظم الحوسبة السحابية الآمنة وتنفيذها وتشغيلها، مع تطوير سياسات السحابة الآمنة.
٣	مصمم معمارية الأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية	تصميم نُظم وشبكات الأمن السيبراني في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية والإشراف على إعداداتها وتطويرها وتنفيذها.
٤	أخصائي البنية التحتية للأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية	فحص وتنصيب وصيانة الأجهزة والبرمجيات المستخدمة للدفاع وحماية الأنظمة والشبكات من التهديدات السيبرانية في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية وتشغيلها والإشراف عليها.

عمليات الأمن السيبراني		
#	الأدوار	الوصف
١	محلل دفاع الأمن السيبراني	استخدام البيانات التي تم استخلاصها من مجموعة أدوات الدفاع السيبراني لتحليل الأحداث الواقعة داخل الجهة بهدف الكشف عن التهديدات والتعامل معها.
٢	أخصائي تقييم الثغرات	تقييم ثغرات النُظم والشبكات، وتحديد مواطن انحرافها عن الإعدادات المقبولة أو السياسات المعمول بها، وقياس فاعلية البنية الدفاعية متعددة الطبقات ضد الثغرات المعروفة.
٣	أخصائي اختبار الاختراقات	أداء محاولات اختراق مصرح لها لأنظمة الحاسبات أو الشبكات أو المنشآت المادية باستخدام أساليب تهديد واقعية لتقييم حالتها الأمنية وكشف الثغرات المحتملة.
٤	أخصائي استجابة للحوادث السيبرانية	مباشرة الحوادث المتعلقة بالأمن السيبراني وتحليلها والاستجابة لها.
٥	أخصائي التحليل الجنائي الرقمي	جمع الأدلة الرقمية وتحليلها، والتحقيق في حوادث الأمن السيبراني لاستخلاص معلومات مفيدة لمعالجة ثغرات النُظم والشبكات.
٦	أخصائي تحقيقات الجرائم السيبرانية	تعريف الأدلة وجمعها وفحصها والحفاظ عليها، باستخدام أساليب تحرٍ واستقصاء موثقة ومقننة.
٧	أخصائي الهندسة العكسية للبرمجيات الضارة	تحليل البرمجيات الضارة (عن طريق تفكيكها وإعادتها إلى صيغة برمجية مفهومة)، وفهم طريقة عملها وتأثيرها وغرضها، وتقديم توصيات للوقاية منها والاستجابة للحوادث الناتجة عنها.
٨	محلل معلومات التهديدات السيبرانية	جمع معلومات عن التهديدات السيبرانية من مصادر مختلفة وتحليلها لتكوين فهم وإدراك عميقين للتهديدات السيبرانية، وخطط المخترقين، والأساليب والخطط المتبعة، لاستنباط وتوثيق مؤشرات من شأنها مساعدة المنظمات في الكشف عن الحوادث السيبرانية والتنبؤ بها، وحماية النُظم والشبكات من التهديدات السيبرانية.
٩	أخصائي اكتشاف التهديدات السيبرانية	البحث الاستباقي عن التهديدات غير المكتشفة في الشبكات والنُظم، وتحديد مؤشرات الاختراق، وتقديم التوصيات للتعامل معها.
١٠	محلل دفاع الأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية	استخدام البيانات، التي تم جمعها من مجموعة متنوعة من أدوات الأمن السيبراني لتحليل الأحداق الواقعة في بيئة أنظمة التحكم

عمليات الأمن السيبراني		
#	الأدوار	الوصف
		الصناعي والتقنيات التشغيلية بهدف الكشف عن تهديدات الأمن السيبراني والتعامل معها.
١١	أخصائي استجابة للحوادث السيبرانية لأنظمة التحكم الصناعي والتقنيات التشغيلية	مباشرة حوادث الأمن السيبراني وتحليلها والاستجابة لها في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية.

أمن تقنية المعلومات		
#	الأدوار	الوصف
١	أخصائي تطوير أمن النظم	تصميم أمن نُظم المعلومات وتطويره واختباره وتقييمه في كافة مراحل تطوير تلك النُظم.
٢	مطور الأمن السيبراني	تطوير برمجيات الأمن السيبراني وتطبيقاته ونُظمه ومنتجاته.
٣	أخصائي البنية التحتية للأمن السيبراني	فحص وتنصيب وصيانة الأجهزة والبرمجيات المستخدمة للدفاع وحماية الأنظمة والشبكات من التهديدات السيبرانية وتشغيلها والإشراف عليها.
٤	أخصائي التشفير	تطوير أنظمة التشفير وخوارزمياته.
٥	أخصائي إدارة الهوية والوصول	إدارة هوية الأفراد والكيانات، وصلاحيات وصولهم إلى الموارد من خلال تطبيق أنظمة، وعمليات التعريف، والتوثيق، والتصريح.
٦	محلل أمن النظم	تطوير أمن النُظم واختباره وصيانته، وتحليل أمن العمليات والأنظمة المدمجة.

مكتب التدقيق الداخلي		
#	الأدوار	الوصف
١	مدقق الأمن السيبراني	تصميم عمليات التدقيق للأمن السيبراني وتنفيذها وإدارتها بهدف تقييم مدى التزام الجهة بالمتطلبات والسياسات والمعايير والضوابط

مكتب التدقيق الداخلي		
#	الأدوار	الوصف
		المعمول بها، وإعداد تقارير التدقيق وتقديمها للأطراف ذات الصلاحية.

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.