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

أدخل شعار الجهة بالضغط على الصورة الموضحة.

نموذج إجراء تقييم الثغرات الأمنية

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.

اختر التصنيف

التاريخ: اضغط هنا لإضافة تاريخ

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

إخلاء المسؤولية

طُوّر 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	عُدِلَ 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

الغرض

يهدف هذا الإجراء إلى تحديد متطلبات الأمن السيبراني التفصيلية المعمول بها لتقييم الثغرات الأمنية وذلك لحماية أصول تقنيات المعلومات لدى <اسم الجهة> من التهديدات والثغرات الأمنية السيبرانية.

تمت مواءمة هذا الإجراء مع متطلبات الأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني، بما في ذلك الضوابط الأساسية للأمن السيبراني (ECC-١:٢٠١٨)، وضوابط الأمن السيبراني للبيانات (DCC-١:٢٠٢٢)، وضوابط الأمن السيبراني للأنظمة الحساسة (CSCC-١:٢٠١٩)، وضوابط الأمن السيبراني للحوسبة السحابية (CCC-١:٢٠٢٠) على سبيل المثال لا الحصر وغيرها من متطلبات الأمن السيبراني التنظيمية والتشريعية ذات العلاقة.

نطاق العمل

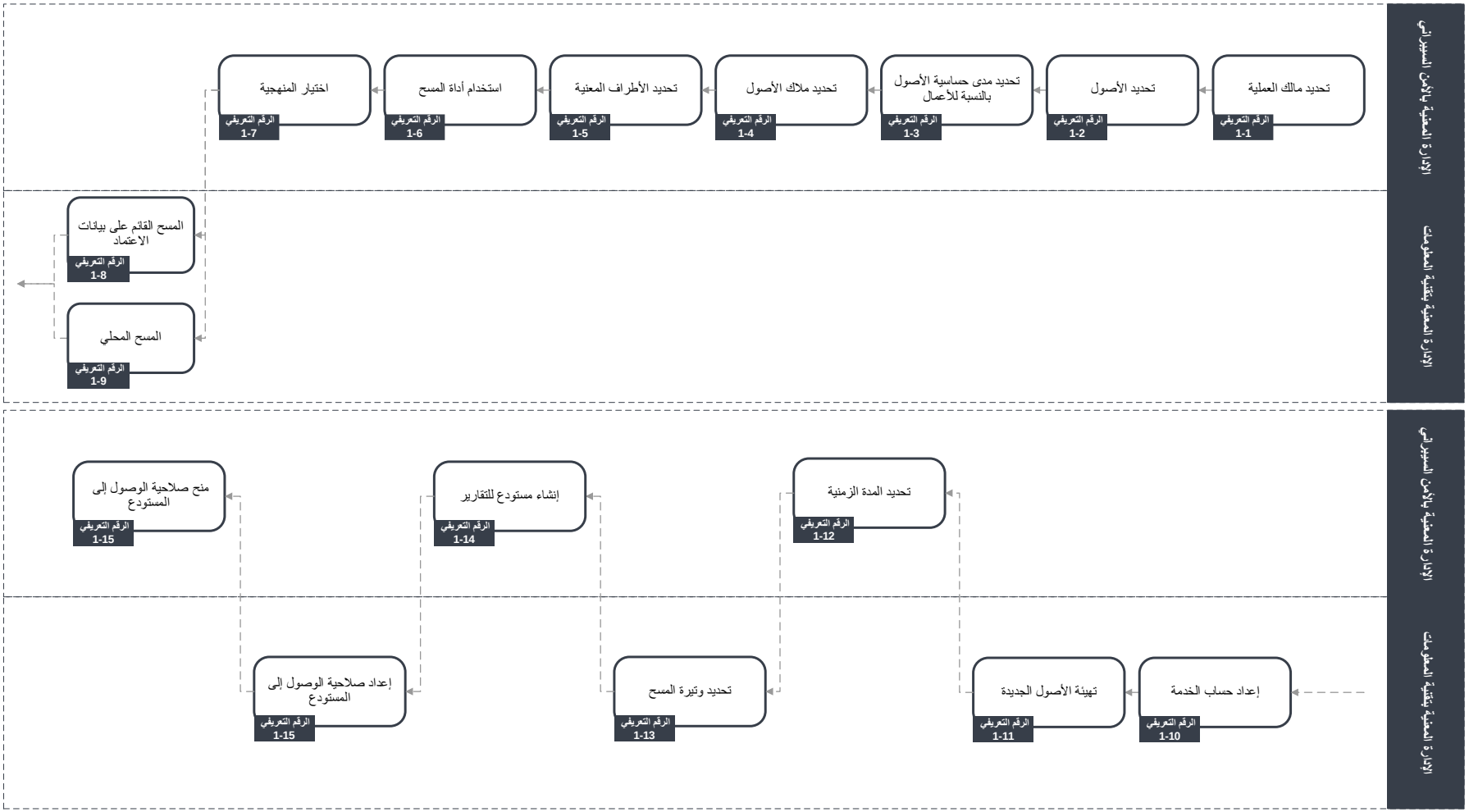
يُطبق هذا الإجراء على جميع أصول تقنية المعلومات الخاصة ب<اسم الجهة> ويُطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

لمحة عامة عن عملية إدارة الثغرات الأمنية

تُقسَّم عملية إدارة الثغرات الأمنية إلى المراحل التالية:

- إعداد تقييم الثغرات الأمنية
- إجراء تقييم الثغرات الأمنية
- معالجة الثغرات الأمنية
- المعلومات الاستباقية عن التهديدات

المرحلة الأولى: إعداد تقييم الثغرات الأمنية



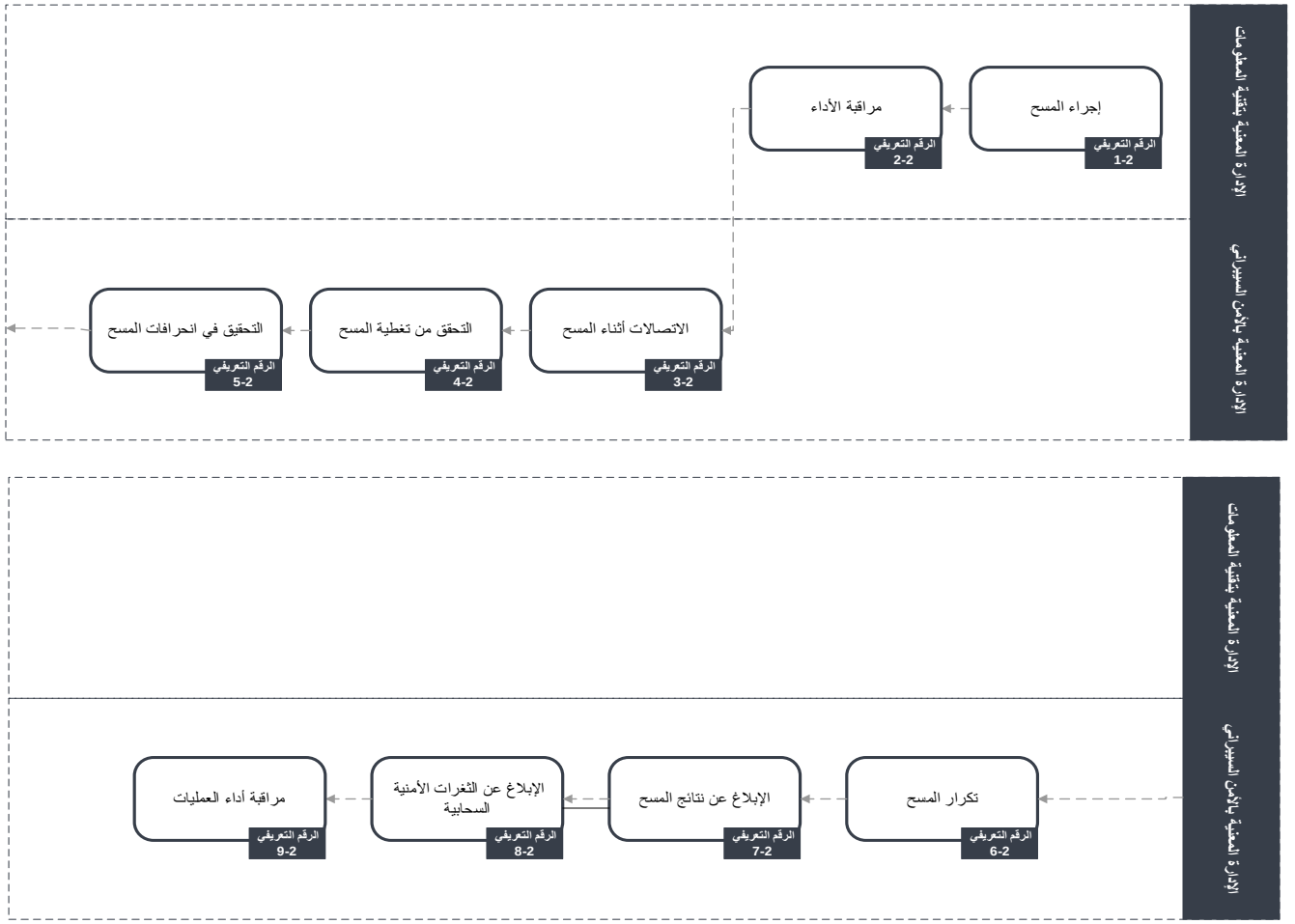
رقم التعريف	الخطوة	الوصف	المالك/المسؤول	المُدخلات	المُخرجات	الأطراف المعنية
١-١	تحديد مالك العملية	تحديد مالك العملية الذي سيتولى مسؤولية تنفيذ وإدارة برنامج إدارة الثغرات الأمنية لدى <اسم الجهة>.	<الإدارة المعنية بالأمن السيبراني>	معايير اختيار مالك العملية	تسمية مالك العملية المكلف بها	<الإدارة المعنية بالأمن السيبراني>
١-٢	تحديد الأصول	تحديد جميع الأصول التي تندرج ضمن نطاق إدارة الثغرات الأمنية. ويتم توثيق الأجهزة والبرمجيات المصرح بها في سياسة ومعيار إدارة الأصول المعلوماتية لدى <اسم الجهة>.	<الإدارة المعنية بالأمن السيبراني>	سجل الأصول المعلوماتية والتقنية	الأصول المحددة ضمن نطاق إدارة الثغرات الأمنية	<الإدارة المعنية بالأمن السيبراني> <الإدارة المعنية بتقنية المعلومات>
١-٣	تحديد مدى حساسية الأصول بالنسبة للأعمال	التحقق من مدى حساسية جميع الأصول التي تندرج ضمن نطاق إدارة الثغرات بالنسبة للأعمال.	<الإدارة المعنية بالأمن السيبراني>	الأصول المحددة ضمن نطاق إدارة الثغرات الأمنية	التحقق من مدى حساسية الأصول بالنسبة للأعمال	<جميع الإدارات في الجهة>
١-٤	تحديد ملاك الأصول	تحديد ملاك أصول الأعمال والأنظمة المسؤولين عن معالجة الثغرات الأمنية المحددة بناءً على مؤشرات الأداء الرئيسية المتفق عليها على النحو الموضح في مؤشرات الأداء الرئيسية لإدارة الثغرات الأمنية لدى <اسم الجهة>.	<الإدارة المعنية بالأمن السيبراني>	التحقق من مدى حساسية الأصول بالنسبة للأعمال	تحديد ملاك أصول الأعمال والأنظمة	<الإدارة المعنية بالأمن السيبراني>
١-٥	تحديد الأطراف المعنية	توثيق الأطراف المعنية المحددة في عملية إدارة الثغرات لدى <اسم الجهة>.	<الإدارة المعنية بالأمن السيبراني>	تحديد ملاك أصول الأعمال والأنظمة	الأطراف المعنية الموثقة	<الإدارة المعنية بالأمن السيبراني>

رقم التعريف	الخطوة	الوصف	المالك/المسؤول	المُدخلات	المُخرجات	الأطراف المعنية
٦-١	استخدام أداة المسح	استخدام أداة مسح الثغرات الأمنية المناسبة للبنية التحتية لشبكة <اسم الجهة>، حتى يمكنها مسح جميع الأصول ضمن نطاق إدارة الثغرات الأمنية.	<الإدارة المعنية بالأمن السيبراني>	التصميم التفصيلي للحل	تطبيق حل مسح الثغرات الأمنية	<الإدارة المعنية بالأمن السيبراني> <الإدارة المعنية بتقنية المعلومات>
٧-١	اختيار المنهجية	اختيار منهجية المسح المناسبة، وذلك من خلال إجراء عملية مسح مصدّق عليها إما باستخدام منهجية المسح القائم على بيانات الاعتماد أو منهجية المسح المحلي (في حالة عدم ملاءمة المسح غير المعتمد وعدم إمكانية استخدام المسح المعتمد بسبب القيود الفنية أو غيرها من القيود)، بالنسبة للأصول الحساسة المحددة.	<الإدارة المعنية بالأمن السيبراني>	التصميم التفصيلي للحل	اختيار منهجية المسح للأصول الحساسة المحددة	<الإدارة المعنية بالأمن السيبراني> <الإدارة المعنية بتقنية المعلومات>
٨-١	إعداد المسح القائم على بيانات الاعتماد	إنشاء الحسابات المستخدمة في المسح القائم على بيانات الاعتماد باتباع سياسة إدارة الصلاحيات الهامة والحساسة لدى <اسم الجهة>.	<الإدارة المعنية بتقنية المعلومات>	اختيار منهجية المسح للأصول الحساسة المحددة	قائمة بالأصول الحساسة التي يمكن الوصول إليها من خلال المسح القائم على بيانات الاعتماد	<الإدارة المعنية بالأمن السيبراني> <الإدارة المعنية بتقنية المعلومات>

رقم التعريف	الخطوة	الوصف	المالك/المسؤول	المُدخلات	المُخرجات	الأطراف المعنية
١-٩	إجراء المسح القائم على بيانات الاعتماد	إجراء المسح القائم على بيانات الاعتماد الاختباري (والمعروف أيضًا باسم "المسح المصدّق عليه") لتقديم قائمة نهائية بالتحديثات والإصلاحات المطلوبة والإعدادات الخاطئة، وذلك باستخدام بيانات الاعتماد لتسجيل الدخول إلى الأنظمة والتطبيقات.	<الإدارة المعنية بتقنية المعلومات>	الحساب المنشأ للمسح القائم على بيانات الاعتماد للأصول الحساسة المحددة	قائمة بالتحديثات والإصلاحات المطلوبة والإعدادات الخاطئة	<الإدارة المعنية بالأمن السيبراني> <الإدارة المعنية بتقنية المعلومات>
١-١٠	إعداد المسح المحلي	تنفيذ المسح المحلي (باستخدام برامج خفيفة ذات بصمة رقمية بسيطة) على الأجهزة المضيفة.	<الإدارة المعنية بتقنية المعلومات>	اختيار منهجية المسح للأصول الحساسة المحددة	قائمة بالأصول الحساسة، مع تنفيذ المسح المحلي	<الإدارة المعنية بالأمن السيبراني> <الإدارة المعنية بتقنية المعلومات>
١-١١	إجراء المسح المحلي	إجراء المسح المحلي الاختباري لجمع البيانات عن الثغرات الأمنية والالتزام والأنظمة، ورفع تلك المعلومات على خادم المسح المركزي لتحليلها.	<الإدارة المعنية بتقنية المعلومات>	تنفيذ المسح المحلي	قائمة بالتحديثات والإصلاحات المطلوبة والإعدادات الخاطئة	<الإدارة المعنية بالأمن السيبراني> <الإدارة المعنية بتقنية المعلومات>
١-١٢	تهيئة الأصول الجديدة	ضمان تهيئة الأصول الجديدة ضمن برنامج إدارة الثغرات الأمنية في الوقت المناسب، بتنفيذ العمليات الضرورية.	<الإدارة المعنية بالأمن السيبراني>	سجل الأصول المحدّث	تهيئة الأصول الجديدة	<الإدارة المعنية بتقنية المعلومات>

رقم التعريف	الخطوة	الوصف	المالك/المسؤول	المُدخلات	المُخرجات	الأطراف المعنية
١-١٣	تحديد المدة الزمنية	التأكد من عدم تداخل مسح الثغرات الأمنية مع أي أنشطة أخرى مجدولة، مثل النسخ الاحتياطي والصيانة المجدولة وما إلى ذلك.	<الإدارة المعنية بتقنية المعلومات>	اختيار منهجية المسح للأصول الحساسة المحددة	التحقق من عدم تداخل المسح مع الأنشطة الأخرى	<الإدارة المعنية بالأمن السيبراني> <الإدارة المعنية بتقنية المعلومات>
١-١٤	تحديد وتيرة المسح	تحديد وتيرة مسح الثغرات الأمنية على النحو المبيّن في سياسة ومعيار إدارة الثغرات الأمنية لدى <اسم الجهة>.	<الإدارة المعنية بالأمن السيبراني>	اختيار منهجية المسح للأصول الحساسة المحددة	تحديد وتيرة مسح الثغرات الأمنية	<الإدارة المعنية بالأمن السيبراني>
١-١٥	إنشاء مستودع للتقارير	إنشاء موقع مركزي لحفظ تقارير مسح الثغرات الأمنية وسجل الثغرات الخاص ب<اسم الجهة>.	<الإدارة المعنية بتقنية المعلومات>	اختيار منهجية المسح للأصول الحساسة المحددة	موقع مركزي لحفظ التقارير	<الإدارة المعنية بالأمن السيبراني> <الإدارة المعنية بتقنية المعلومات>
١-١٦	منح صلاحية الوصول إلى المستودع	ضمان عدم منح صلاحية الوصول إلى هذا الموقع المركزي إلا للموظفين على أساس الحاجة المشروعة إلى المعرفة كما هو موضح في سياسة إدارة الثغرات الأمنية لدى <اسم الجهة>.	<الإدارة المعنية بالأمن السيبراني>	قائمة بالموظفين بصلاحية الوصول إلى الموقع المركزي	نموذج صلاحيات الوصول إلى المستودع المركزي بحسب الأدوار	<الإدارة المعنية بالأمن السيبراني> <الإدارة المعنية بتقنية المعلومات>

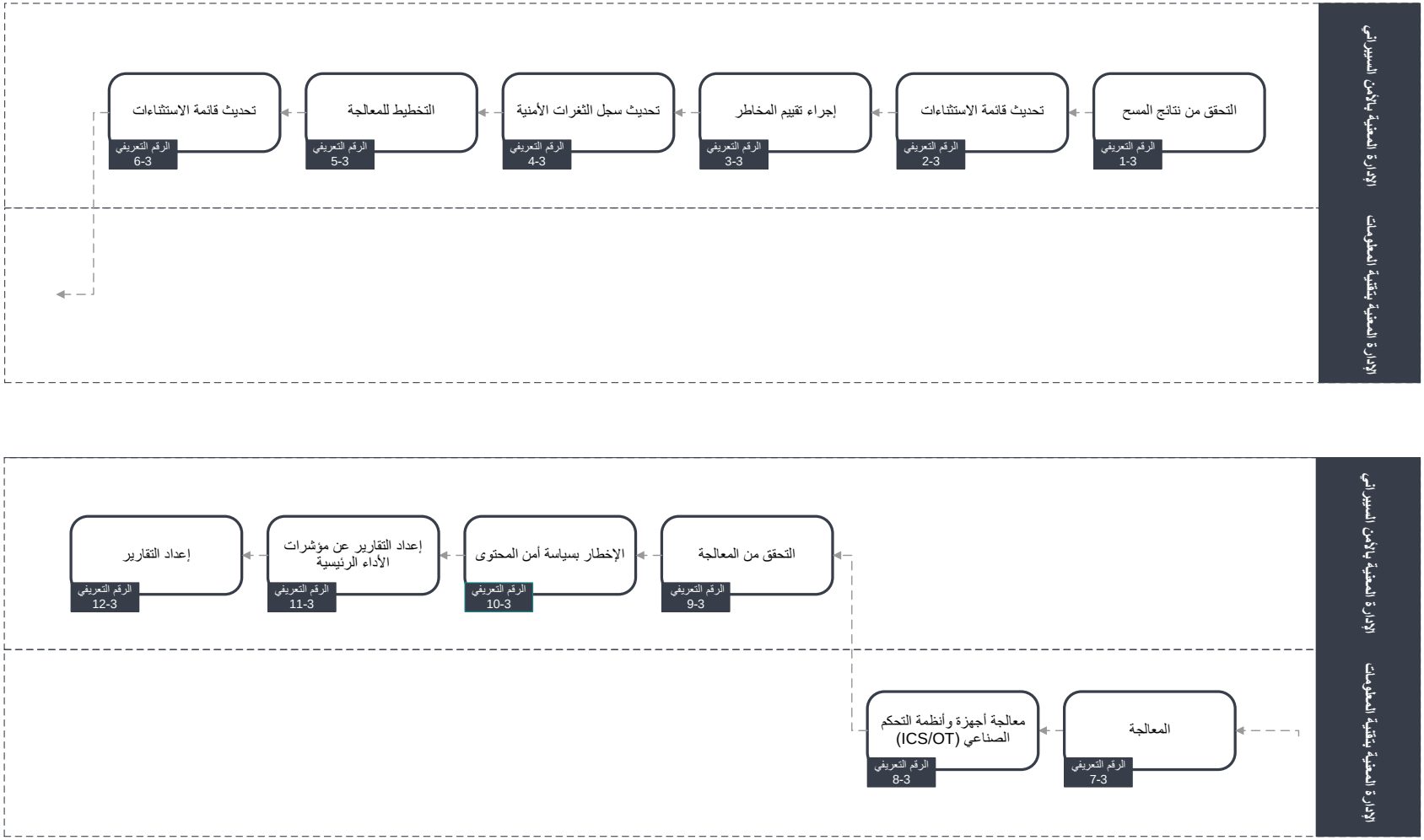
المرحلة الثانية: إجراء تقييم الثغرات الأمنية



رقم التعريف	الخطوة	الوصف	المالك/المسؤول	المُدخلات	المُخرجات	الأطراف المعنية
٢-١	إجراء المسح	إجراء مسح الثغرات الأمنية كما هو موثق في سجل التغييرات المعتمد.	<الإدارة المعنية بتقنية المعلومات>	سجل التغييرات المعتمد	تقرير مسح الثغرات الأمنية	<الإدارة المعنية بالأمن السيبراني> <الإدارة المعنية بتقنية المعلومات>
٢-٢	مراقبة الأداء	مراقبة أداء كلٍّ من بيئة مسح الثغرات الأمنية والأصول الجاري مسحها طوال مدة المسح.	<الإدارة المعنية بتقنية المعلومات>	تحديد الأصول الحساسة ضمن نطاق مسح الثغرات الأمنية	الأصول المتأثرة سلبيًا بالمسح	<الإدارة المعنية بالأمن السيبراني> <الإدارة المعنية بتقنية المعلومات>
٢-٣	الاتصالات أثناء المسح	إبلاغ الأطراف المعنية ذات العلاقة بأي مشكلة على النحو المبين في سجل التغييرات.	<الإدارة المعنية بالأمن السيبراني>	الأصول المتأثرة سلبيًا بالمسح	إبلاغ الأطراف المعنية بالمشكلة	<جميع الإدارات في الجهة>
٢-٤	التحقق من تغطية المسح	التحقق من مسح جميع الأصول المشمولة ضمن نطاق إدارة الثغرات الأمنية بنجاح.	<الإدارة المعنية بالأمن السيبراني>	تقرير مسح الثغرات الأمنية، سجل الأصول	قائمة بالأصول التي لم يتم مسحها خلال مسح الثغرات الأمنية	<الإدارة المعنية بالأمن السيبراني> <الإدارة المعنية بتقنية المعلومات>

رقم التعريف	الخطوة	الوصف	المالك/المسؤول	المُدخلات	المُخرجات	الأطراف المعنية
٢-٥	التحقيق في الاختلافات	التحقيق في أي اختلاف في الوقت المناسب بناءً على مؤشرات الأداء الرئيسية المتفق عليها.	<الإدارة المعنية بالأمن السيبراني>	قائمة بالأصول التي لم يتم مسحها خلال مسح الثغرات الأمنية	التحقيق في الاختلافات	<الإدارة المعنية بالأمن السيبراني>
٢-٦	تكرار المسح	تكرار مسح الثغرات الأمنية على الأصول في حالة فشل المسح خلال المحاولة السابقة.	<الإدارة المعنية بالأمن السيبراني>	قائمة بالأصول التي لم يتم مسحها خلال مسح الثغرات الأمنية	المسح المُكرّر	<الإدارة المعنية بالأمن السيبراني> <الإدارة المعنية بتقنية المعلومات>
٢-٧	الإبلاغ عن نتائج المسح	إبلاغ الأطراف المعنية بالنتيجة النهائية للمسح.	<الإدارة المعنية بالأمن السيبراني>	تقرير مسح الثغرات الأمنية	إتاحة نتيجة المسح على المستودع المركزي	<الإدارة المعنية بالأمن السيبراني>
٢-٨	الإبلاغ عن الثغرات الأمنية السحابية	إبلاغ فريق الخدمات السحابية (Cloud Service Team) بالثغرات المحددة التي قد تؤثر عليه ووضع تدابير الحماية المطلوبة.	<الإدارة المعنية بالأمن السيبراني>	إتاحة نتيجة المسح على المستودع المركزي	الإبلاغ عن الثغرات في الخدمات السحابية	<الإدارة المعنية بالأمن السيبراني>
٢-٩	مراقبة أداء العمليات	قياس مؤشرات الأداء الرئيسية لضمان التحسين المستمر لإدارة الثغرات الأمنية.	<الإدارة المعنية بالأمن السيبراني>	تقرير مسح الثغرات الأمنية	تقرير مؤشرات الأداء الرئيسية	<الإدارة المعنية بالأمن السيبراني>

المرحلة الثالثة: معالجة الثغرات الأمنية

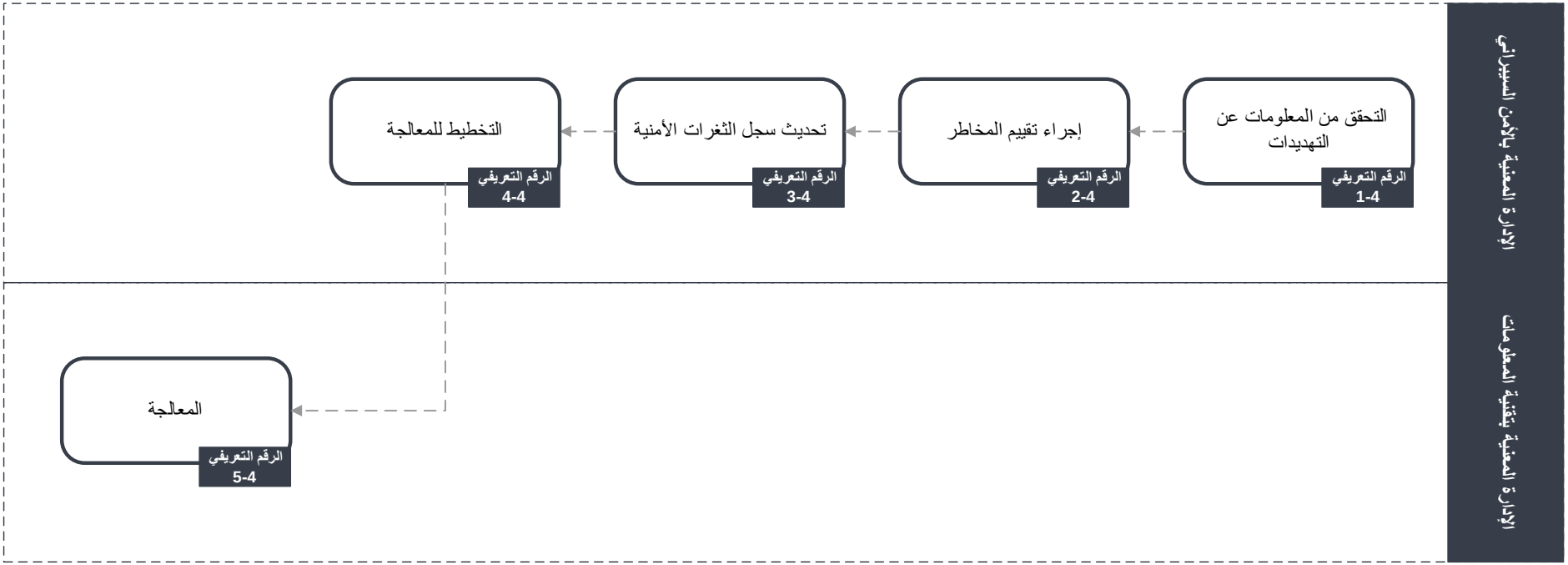


رقم التعريف	المهمة	الوصف	المالك/المسؤول	المُدخلات	المُخرجات	الأطراف المعنية
٣-١	التحقق من نتائج المسح	التحقق من نتائج مسح الثغرات الأمنية.	<الإدارة المعنية بالأمن السيبراني>	تقرير مسح الثغرات الأمنية	التحقق من النتائج النهائية	<الإدارة المعنية بالأمن السيبراني>
٣-٢	تحديث قائمة الاستثناءات	إضافة التنبيهات الكاذبة إلى قائمة الاستثناءات.	<الإدارة المعنية بالأمن السيبراني>	التحقق من النتائج النهائية	إضافة التنبيهات الكاذبة إلى قائمة الاستثناءات.	<الإدارة المعنية بالأمن السيبراني><الإدارة المعنية بتقنية المعلومات>
٣-٣	إجراء تقييم المخاطر	تحليل الثغرات الأمنية والمخاطر المرتبطة بها بناءً على سياسة إدارة المخاطر لدى <اسم الجهة>.	<الإدارة المعنية بالأمن السيبراني>	التحقق من النتائج النهائية	تحليل الثغرات الأمنية والمخاطر	<الإدارة المعنية بالأمن السيبراني>
٣-٤	تحديث سجل الثغرات الأمنية	توثيق جميع الثغرات المحددة في سجل الثغرات الأمنية الخاص ب<اسم الجهة>.	<الإدارة المعنية بالأمن السيبراني>	تحليل الثغرات الأمنية والمخاطر	سجل الثغرات الأمنية المحدّث	<الإدارة المعنية بالأمن السيبراني>
٣-٥	التخطيط للمعالجة	تحديد الإجراءات التصحيحية لكل ثغرة أمنية محددة بناءً على مستوى خطورتها.	<الإدارة المعنية بالأمن السيبراني>	سجل الثغرات الأمنية المحدّث	خطة العمل المحددة لتقييم الثغرات الأمنية	<الإدارة المعنية بالأمن السيبراني>
٣-٦	تحديث قائمة الاستثناءات	إضافة الثغرات ذات المستوى المقبول من المخاطر إلى قائمة الاستثناءات.	<الإدارة المعنية بالأمن السيبراني>	سجل الثغرات الأمنية المحدّث	قائمة الاستثناءات المحدّثة	<الإدارة المعنية بالأمن السيبراني>

رقم التعريف	المهمة	الوصف	المالك/المسؤول	المُدخلات	المُخرجات	الأطراف المعنية
٣-٧	المعالجة	تنفيذ الإجراءات التصحيحية وفقًا لسياسة ومعيار إدارة التحديثات والإصلاحات لدى <اسم الجهة>.	<الإدارة المعنية بتقنية المعلومات>	خطة العمل المحددة لتقييم الثغرات الأمنية	تنفيذ الإجراءات التصحيحية	<الإدارة المعنية بالأمن السيبراني> <الإدارة المعنية بتقنية المعلومات>
٣-٨	معالجة أجهزة وأنظمة التحكم الصناعي (OT/ICS)	معالجة الثغرات الأمنية الحرجة المكتشفة حديثًا ذات المخاطر الكبيرة على بيئة أجهزة وأنظمة التحكم الصناعي (OT/ICS) بطريقة آمنة.	<الإدارة المعنية بتقنية المعلومات>	خطة العمل المحددة لتقييم الثغرات الأمنية	تنفيذ الإجراءات التصحيحية	<الإدارة المعنية بالأمن السيبراني> <الإدارة المعنية بتقنية المعلومات>
٣-٩	التحقق من المعالجة	التحقق من نجاح تنفيذ الإجراءات التصحيحية من خلال إجراء مسح للثغرات الأمنية على الأصول ذات الصلة.	<الإدارة المعنية بالأمن السيبراني>	تنفيذ الإجراءات التصحيحية	التحقق من التنفيذ	<الإدارة المعنية بالأمن السيبراني> <الإدارة المعنية بتقنية المعلومات>
٣-١٠	الإشعار بسياسة أمن المحتوى	إخطار الإدارة بسياسة أمن المحتوى (Content Security Policy) وباتخاذ تدابير الحماية من الثغرات الأمنية السحابية.	<الإدارة المعنية بالأمن السيبراني>	التحقق من التنفيذ	الإبلاغ بنتيجة التنفيذ	<الإدارة المعنية بالأمن السيبراني>

رقم التعريف	المهمة	الوصف	المالك/المسؤول	المُدخلات	المُخرجات	الأطراف المعنية
٣-١١	إعداد التقارير عن مؤشرات الأداء الرئيسية	قياس مؤشرات الأداء الرئيسية المحددة في قسم مؤشرات الأداء الرئيسية من الوثيقة لضمان التحسين المستمر لإدارة الثغرات الأمنية.	<الإدارة المعنية بالأمن السيبراني>	التحقق من التنفيذ	تقرير مؤشرات الأداء الرئيسية	<الإدارة المعنية بالأمن السيبراني>
٣-١٢	إعداد التقارير	رفع تقارير منتظمة إلى الإدارة العليا ل<اسم الجهة> عن الثغرات الأمنية والمخاطر المرتبطة بها كما هو موضح في سياسة إدارة المخاطر لدى <اسم الجهة> .	<الإدارة المعنية بالأمن السيبراني>	تقرير مؤشرات الأداء الرئيسية	رفع تقارير منتظمة إلى الإدارة العليا	<الإدارة المعنية بالأمن السيبراني>

المرحلة الرابعة: المعلومات الاستباقية عن التهديدات



رقم التعريف	المهمة	الوصف	المالك/المسؤول	المُدخلات	المُخرجات	الأطراف المعنية
١-٤	التحقق من المعلومات عن التهديدات	المراجعة اليومية للثغرات الفنية المحتملة الصادرة عن المصادر الموثوقة المصرح بها.	<الإدارة المعنية بالأمن السيبراني>	المعلومات من المصادر الموثوقة	التحقق من النتائج النهائية	<الإدارة المعنية بالأمن السيبراني>

رقم التعريف	المهمة	الوصف	المالك/المسؤول	المُدخلات	المُخرجات	الأطراف المعنية
٤-٢	إجراء تقييم المخاطر	تحليل الثغرات الأمنية والمخاطر المرتبطة بها بناءً على سياسة إدارة المخاطر لدى <اسم الجهة>.	<الإدارة المعنية بالأمن السيبراني>	التحقق من النتائج النهائية	تحليل الثغرات الأمنية والمخاطر	<الإدارة المعنية بالأمن السيبراني>
٤-٣	تحديث سجل الثغرات الأمنية	توثيق جميع الثغرات المحددة في سجل الثغرات الأمنية الخاص ب<اسم الجهة>.	<الإدارة المعنية بالأمن السيبراني>	تحليل الثغرات الأمنية والمخاطر	سجل الثغرات الأمنية المحدّث	<الإدارة المعنية بالأمن السيبراني>
٤-٤	التخطيط للمعالجة	تحديد الإجراءات التصحيحية لكل ثغرة أمنية محددة بناءً على مستوى خطورتها.	<الإدارة المعنية بالأمن السيبراني>	سجل الثغرات الأمنية المحدّث	خطة العمل المحددة لتقييم الثغرات الأمنية	<الإدارة المعنية بالأمن السيبراني>
٤-٥	المعالجة	تنفيذ الإجراءات التصحيحية بناءً على سياسة ومعيار إدارة التحديثات والإصلاحات لدى <اسم الجهة>.	<الإدارة المعنية بتقنية المعلومات>	خطة العمل المحددة لتقييم الثغرات الأمنية	تنفيذ الإجراءات التصحيحية	<الإدارة المعنية بتقنية المعلومات>

الأدوار والمسؤوليات

١- **مالك الإجراء**: <رئيس الإدارة المعنية بالأمن السيبراني>

٢- **مراجعة الإجراء وتحديثه:** <الإدارة المعنية بالأمن السيبراني>

٣- **تنفيذ الإجراء وتطبيقه**: <الإدارة المعنية بتقنية المعلومات>

٤- **قياس الالتزام بالإجراء:** <الإدارة المعنية بالأمن السيبراني>

التحديث والمراجعة

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

الالتزام بالإجراء

١- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> التأكد من التزام <اسم الجهة> بهذا الإجراء دوريًا.

٢- يطبق هذا الإجراء على جميع أنظمة وخوادم <اسم الجهة> وعلى جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

٣- قد يعرّض أي انتهاك لهذا الإجراء صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في <اسم الجهة>.