قائمة مراجعة التحضير للاستجابة للحوادث السيبرانية

Incident Response Preparation Checklist

1. السياسات والإجراءات / Policies and Procedures

1.1 خطة الاستجابة للحوادث / Incident Response Plan

- [ ] تم وضع خطة شاملة للاستجابة للحوادث
- [ ] تم تحديد أدوار ومسؤوليات كل عضو في الفريق
- [ ] تم تحديد إجراءات التصعيد والإبلاغ
- [ ] تم وضع معايير تصنيف الحوادث
- [ ] تم تحديد جهات الاتصال الداخلية والخارجية
- [ ] تم مراجعة وتحديث الخطة خلال الـ12 شهر الماضية

1.2 السياسات الأمنية / Security Policies

- [ ] سياسة أمن المعلومات محدثة ومعتمدة
- [ ] سياسة استخدام الأنظمة والشبكات
- [ ] سياسة إدارة كلمات المرور
- [ ] سياسة النسخ الاحتياطي والاستعادة
- [ ] سياسة التعامل مع الحوادث الأمنية
- [ ] سياسة الوصول للأنظمة والبيانات

2. تشكيل فريق الاستجابة / Incident Response Team Formation

2.1 أعضاء الفريق الأساسيين / Core Team Members

- [ ] مدير فريق الاستجابة (Incident Commander)

- [ ] محلل الأمن السيبراني (Security Analyst)
- [ ] مدير الأنظمة (System Administrator)
- [ ] مدير الشبكات (Network Administrator)
- [ ] محلل الطب الشرعي الرقمي (Digital Forensics Analyst)
- [ ] ممثل الشؤون القانونية (Legal Representative)
- [ ] ممثل العلاقات العامة (PR Representative)

2.2 معلومات الاتصال / Contact Information

- [ ] قائمة اتصال محدثة لجميع أعضاء الفريق
- [ ] أرقام هواتف الطوارئ متاحة 24/7
- [ ] عناوين بريد إلكتروني بديلة
- [ ] وسائل اتصال آمنة ومشفرة
- [ ] معلومات اتصال الجهات الخارجية (الشرطة، المحامين، إلخ)

3. التدريب والتأهيل / Training and Qualification

3.1 تدريب الفريق / Team Training

- [ ] تدريب أساسي على الاستجابة للحوادث لجميع الأعضاء
- [ ] تدريب متخصص للمحللين الأمنيين
- [ ] تدريب على استخدام أدوات التحليل الجنائي
- [ ] تدريب على التعامل مع وسائل الإعلام
- [ ] تدريب على الجوانب القانونية للحوادث السيبرانية

3.2 التمارين والمحاكاة / Exercises and Simulations

- [ ] تمارين سطح المكتب (Tabletop Exercises) ربع سنوية
- [ ] محاكاة حوادث واقعية سنوياً
- [ ] اختبار خطط الطوارئ والنسخ الاحتياطي
- [ ] تقييم أداء الفريق بعد كل تمرين
- [ ] تحديث الخطط بناءً على نتائج التمارين

4. الأدوات والتقنيات / Tools and Technologies

4.1 أدوات المراقبة / Monitoring Tools

- [ ] نظام SIEM مُعد ومُحدث
- [ ] أدوات EDR على جميع نقاط النهاية
- [ ] أنظمة IDS/IPS مُفعلة ومُراقبة
- [ ] أدوات مراقبة الشبكة
- [ ] نظام مراقبة السجلات (Log Management)
- [ ] أدوات تحليل التهديدات (Threat Intelligence)

4.2 أدوات التحليل الجنائي / Forensic Tools

- [ ] أدوات تحليل الذاكرة (Memory Analysis)
- [ ] أدوات تحليل القرص الصلب (Disk Analysis)
- [ ] أدوات تحليل الشبكة (Network Analysis)
- [ ] أدوات استخراج وتحليل السجلات
- [ ] بيئة معزولة للتحليل الآمن
- [ ] أدوات توثيق الأدلة الرقمية

4.3 أدوات الاتصال والتنسيق / Communication Tools

- [ ] نظام تذاكر لتتبع الحوادث
- [ ] أدوات اتصال آمنة ومشفرة
- [ ] منصة مشاركة المعلومات الآمنة
- [ ] أدوات التعاون عن بُعد
- [ ] نظام إشعارات الطوارئ

5. البنية التحتية / Infrastructure

5.1 الشبكة والأنظمة / Network and Systems

- [ ] تجزئة الشبكة (Network Segmentation)
- [ ] نقاط مراقبة الشبكة (Network Monitoring Points)

- [ ] أنظمة النسخ الاحتياطي تعمل بانتظام
- [ ] خطة استمرارية العمل مُحدثة
- [ ] بيئة اختبار منفصلة
- [ ] إجراءات الاستعادة السريعة

5.2 الأمان المادي / Physical Security

- [ ] حماية مراكز البيانات
- [ ] كاميرات مراقبة وأنظمة إنذار
- [ ] تحكم في الوصول للمناطق الحساسة
- [ ] حماية الأجهزة المحمولة
- [ ] إجراءات التخلص الآمن من الأجهزة

6. التوثيق والسجلات / Documentation and Records

6.1 الوثائق الأساسية / Essential Documents

- [ ] خطة الاستجابة للحوادث محدثة
- [ ] إجراءات التشغيل القياسية (SOPs)
- [ ] قوائم مراجعة للحوادث المختلفة
- [ ] نماذج الإبلاغ والتوثيق
- [ ] معلومات الاتصال الطارئة
- [ ] خرائط الشبكة والأنظمة

6.2 إدارة السجلات / Log Management

- [ ] سياسة الاحتفاظ بالسجلات محددة
- [ ] تجميع السجلات من جميع المصادر
- [ ] مزامنة الوقت عبر جميع الأنظمة
- [ ] حماية سلامة السجلات
- [ ] نسخ احتياطية منتظمة للسجلات

7. العلاقات الخارجية / External Relationships

7.1 الجهات الحكومية / Government Agencies

- [ ] معلومات اتصال الجهات التنظيمية
- [ ] إجراءات الإبلاغ الإلزامي
- [ ] علاقة مع جهات إنفاذ القانون
- [ ] تنسيق مع مراكز الاستجابة الوطنية

7.2 الشركاء والموردين / Partners and Vendors

- [ ] اتفاقيات مستوى الخدمة (SLAs) محدثة
- [ ] معلومات اتصال الدعم الفني
- [ ] إجراءات التصعيد مع الموردين
- [ ] خطط الطوارئ مع الشركاء

8. الاختبار والتحقق / Testing and Validation

8.1 اختبارات دورية / Regular Testing

- [ ] اختبار أنظمة النسخ الاحتياطي شهرياً
- [ ] اختبار إجراءات الاستعادة ربع سنوياً
- [ ] اختبار أدوات المراقبة والإنذار
- [ ] اختبار قنوات الاتصال الطارئة
- [ ] مراجعة وتحديث الوثائق

8.2 تقييم الجاهزية / Readiness Assessment

- [ ] تقييم شامل للجاهزية سنوياً
- [ ] مراجعة خارجية للخطط والإجراءات
- [ ] قياس أوقات الاستجابة
- [ ] تقييم فعالية التدريب
- [ ] مراجعة الدروس المستفادة من الحوادث السابقة

9. الامتثال والمعايير / Compliance and Standards

9.1 المعايير الدولية / International Standards

- [ ] الامتثال لمعايير ISO 27035
- [ ] تطبيق إطار عمل NIST
- [ ] اتباع أفضل الممارسات الدولية
- [ ] مراجعة التحديثات على المعايير

9.2 المتطلبات التنظيمية / Regulatory Requirements

- [ ] الامتثال للقوانين المحلية
- [ ] متطلبات حماية البيانات الشخصية
- [ ] متطلبات الإبلاغ عن الحوادث
- [ ] متطلبات الاحتفاظ بالسجلات

10. المراجعة والتحسين المستمر / Review and Continuous Improvement

10.1 المراجعة الدورية / Regular Review

- [ ] مراجعة شهرية لأداء الفريق
- [ ] مراجعة ربع سنوية للخطط والإجراءات
- [ ] مراجعة سنوية شاملة للبرنامج
- [ ] تحديث الخطط بناءً على التهديدات الجديدة

10.2 التحسين المستمر / Continuous Improvement

- [ ] تحليل الحوادث السابقة واستخلاص الدروس
- [ ] تطوير الإجراءات بناءً على التجارب
- [ ] تحديث التدريب والمهارات
- [ ] مواكبة التطورات التقنية والتهديدات الجديدة

تاريخ المراجعة الأخيرة: __
المراجع التالي المقرر: __
المسؤول عن المراجعة: ___

ملاحظات: