مصفوفة الأدوار والمسؤوليات في الاستجابة للحوادث السيبرانية

Incident Response Roles and Responsibilities Matrix

---

1. هيكل فريق الاستجابة / Incident Response Team Structure

الفريق الأساسي / Core Team

- 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

الفريق الداعم / Support Team

- ممثل الشؤون القانونية / Legal Representative
- ممثل العلاقات العامة / PR Representative
- مدير الموارد البشرية / HR Manager
- مدير أمن المعلومات / Information Security Manager
- ممثل الإدارة العليا / Senior Management Representative

---

2. مصفوفة الأدوار والمسؤوليات / Roles and Responsibilities Matrix

---

مدير فريق الاستجابة / Incident Commander

المسؤوليات الأساسية / Primary Responsibilities

- [ ] **القيادة العامة للاستجابة / Overall Response Leadership**
- تنسيق جميع أنشطة الاستجابة
- اتخاذ القرارات الاستراتيجية
- تحديد أولويات الاستجابة
- إدارة الموارد والفريق
- [ ] **التواصل والإبلاغ / Communication and Reporting**
- إبلاغ الإدارة العليا
- التنسيق مع الجهات الخارجية
- إعداد التقارير الدورية
- إدارة التواصل مع وسائل الإعلام
- [ ] **إدارة الأزمات / Crisis Management**
- تقييم مستوى الخطورة
- تحديد استراتيجية الاستجابة
- إدارة الضغوط والتوقعات
- اتخاذ قرارات التصعيد

المهارات المطلوبة / Required Skills

- خبرة في إدارة الأزمات
- مهارات قيادية قوية
- معرفة تقنية شاملة
- مهارات تواصل ممتازة

معلومات الاتصال / Contact Information

- الاسم / Name: ___
- الهاتف الأساسي / Primary Phone: ___
- الهاتف البديل / Backup Phone: ___
- البريد الإلكتروني / Email: ___

محلل الأمن السيبراني / Security Analyst

المسؤوليات الأساسية / Primary Responsibilities

- [ ] **التحليل الأمني / Security Analysis**
- تحليل التهديدات والثغرات
- تقييم مستوى الخطورة
- تحديد نوع الهجوم
- تحليل المؤشرات الأمنية
- [ ] **المراقبة والكشف / Monitoring and Detection**
- مراقبة أنظمة الأمان
- تحليل التنبيهات الأمنية
- البحث عن مؤشرات الاختراق
- تتبع أنشطة المهاجمين
- [ ] **التوثيق والتقارير / Documentation and Reporting**
- توثيق النتائج التقنية
- إعداد تقارير التحليل
- تحديث قواعد بيانات التهديدات
- مشاركة المعلومات الأمنية

المهارات المطلوبة / Required Skills

- خبرة في الأمن السيبراني

- معرفة بأنواع التهديدات
- مهارات التحليل التقني
- خبرة في أدوات الأمان

معلومات الاتصال / Contact Information

- الاسم / Name: ___
- الهاتف الأساسي / Primary Phone: ___
- الهاتف البديل / Backup Phone: ___
- البريد الإلكتروني / Email: ___

مدير الأنظمة / System Administrator

المسؤوليات الأساسية / Primary Responsibilities

- [ ] **إدارة الأنظمة / System Management**
- مراقبة حالة الأنظمة
- تنفيذ إجراءات الاحتواء
- إصلاح الأنظمة المتأثرة
- استعادة الخدمات
- [ ] **النسخ الاحتياطي والاستعادة / Backup and Recovery**
- إدارة النسخ الاحتياطية
- استعادة البيانات
- اختبار سلامة النسخ
- تنفيذ خطط الاستعادة
- [ ] **التحديث والصيانة / Updates and Maintenance**
- تطبيق التحديثات الأمنية
- إصلاح الثغرات
- تحديث التكوينات
- صيانة الأنظمة

المهارات المطلوبة / Required Skills

- خبرة في إدارة الأنظمة
- معرفة بأنظمة التشغيل
- مهارات استكشاف الأخطاء
- خبرة في النسخ الاحتياطي

معلومات الاتصال / Contact Information

- الاسم / Name: ___
- الهاتف الأساسي / Primary Phone: ___
- الهاتف البديل / Backup Phone: ___
- البريد الإلكتروني / Email: ___

مدير الشبكات / Network Administrator

المسؤوليات الأساسية / Primary Responsibilities

- [ ] **إدارة الشبكة / Network Management**
- مراقبة حركة الشبكة
- تحليل السجلات الشبكية
- تنفيذ إجراءات العزل
- إدارة الجدران النارية
- [ ] **الأمان الشبكي / Network Security**
- تحديث قواعد الأمان
- مراقبة التهديدات الشبكية
- تنفيذ إجراءات الحماية
- تحليل حركة البيانات المشبوهة
- [ ] **الاستعادة والإصلاح / Recovery and Repair**
- إصلاح الاتصالات الشبكية

- استعادة الخدمات الشبكية
- اختبار الاتصالات
- تحسين الأداء الشبكي

المهارات المطلوبة / Required Skills

- خبرة في إدارة الشبكات
- معرفة ببروتوكولات الشبكة
- مهارات تحليل حركة البيانات
- خبرة في أمان الشبكات

معلومات الاتصال / Contact Information

- الاسم / Name: ___
- الهاتف الأساسي / Primary Phone: ___
- الهاتف البديل / Backup Phone: ___
- البريد الإلكتروني / Email: ___

محلل الطب الشرعي الرقمي / Digital Forensics Analyst

المسؤوليات الأساسية / Primary Responsibilities

- [ ] **جمع الأدلة / Evidence Collection**
- جمع الأدلة الرقمية
- حفظ سلامة الأدلة
- توثيق سلسلة الحفظ
- أخذ لقطات للأنظمة
- [ ] **التحليل الجنائي / Forensic Analysis**
- تحليل الأدلة الرقمية
- استخراج البيانات المحذوفة
- تحليل البرمجيات الخبيثة

- تتبع أنشطة المهاجمين
- [ ] **التقارير القانونية / Legal Reporting**
- إعداد التقارير الجنائية
- توثيق النتائج للمحاكم
- التعاون مع المحققين
- تقديم الشهادات الخبيرة

المهارات المطلوبة / Required Skills

- خبرة في الطب الشرعي الرقمي
- معرفة بأدوات التحليل الجنائي
- مهارات التحليل التقني
- معرفة بالإجراءات القانونية

معلومات الاتصال / Contact Information

- الاسم / Name: ___
- الهاتف الأساسي / Primary Phone: ___
- الهاتف البديل / Backup Phone: ___
- البريد الإلكتروني / Email: ___

ممثل الشؤون القانونية / Legal Representative

المسؤوليات الأساسية / Primary Responsibilities

- [ ] **الاستشارات القانونية / Legal Consultation**
- تقديم المشورة القانونية
- تحديد المتطلبات القانونية
- تقييم المخاطر القانونية
- إدارة القضايا القانونية
- [ ] **الامتثال التنظيمي / Regulatory Compliance**

- ضمان الامتثال للقوانين
- إدارة متطلبات الإبلاغ
- التنسيق مع الجهات التنظيمية
- إدارة التحقيقات الرسمية
- [ ] **إدارة المخاطر / Risk Management**
- تقييم المخاطر القانونية
- إدارة دعاوى التعويض
- التفاوض مع الأطراف المتضررة
- حماية حقوق المؤسسة

المهارات المطلوبة / Required Skills

- خبرة قانونية في الأمن السيبراني
- معرفة بقوانين حماية البيانات
- مهارات التفاوض
- خبرة في إدارة المخاطر

معلومات الاتصال / Contact Information

- الاسم / Name: ___
- الهاتف الأساسي / Primary Phone: ___
- الهاتف البديل / Backup Phone: ___
- البريد الإلكتروني / Email: ___

ممثل العلاقات العامة / PR Representative

المسؤوليات الأساسية / Primary Responsibilities

- [ ] **إدارة التواصل / Communication Management**
- إعداد البيانات الصحفية
- إدارة التواصل مع الإعلام
- تنسيق الرسائل العامة

- إدارة وسائل التواصل الاجتماعي
- [ ] **إدارة السمعة / Reputation Management**
- حماية سمعة المؤسسة
- إدارة الأزمات الإعلامية
- تصحيح المعلومات الخاطئة
- بناء الثقة مع الجمهور
- [ ] **التواصل مع أصحاب المصلحة / Stakeholder Communication**
- التواصل مع العملاء
- إبلاغ الشركاء
- تحديث المساهمين
- إدارة توقعات الجمهور

المهارات المطلوبة / Required Skills

- خبرة في العلاقات العامة
- مهارات التواصل الممتازة
- خبرة في إدارة الأزمات
- معرفة بوسائل الإعلام

معلومات الاتصال / Contact Information

- الاسم / Name: ___
- الهاتف الأساسي / Primary Phone: ___
- الهاتف البديل / Backup Phone: ___
- البريد الإلكتروني / Email: ___

---

3. مصفوفة اتخاذ القرارات / Decision Making Matrix

مستويات التصعيد / Escalation Levels

المستوى الأول - حوادث منخفضة الخطورة / Level 1 - Low Severity

صلاحيات اتخاذ القرار: - محلل الأمن السيبراني - مدير الأنظمة - مدير الشبكات

القرارات المسموحة: - إجراءات الاحتواء الأساسية - إعادة تشغيل الخدمات - تطبيق التحديثات الأمنية

المستوى الثاني - حوادث متوسطة الخطورة / Level 2 - Medium Severity

صلاحيات اتخاذ القرار: - مدير فريق الاستجابة - مدير أمن المعلومات

القرارات المسموحة: - إيقاف الخدمات المتأثرة - تفعيل خطط الطوارئ - الإبلاغ الخارجي المحدود

المستوى الثالث - حوادث عالية الخطورة / Level 3 - High Severity

صلاحيات اتخاذ القرار: - الإدارة العليا - مدير فريق الاستجابة

القرارات المسموحة: - إيقاف العمليات الحرجة - تفعيل مركز الأزمات - الإبلاغ الرسمي للجهات

المستوى الرابع - حوادث حرجة / Level 4 - Critical Severity

صلاحيات اتخاذ القرار: - الرئيس التنفيذي - مجلس الإدارة

القرارات المسموحة: - إعلان حالة الطوارئ - تفعيل خطط استمرارية العمل - اتخاذ قرارات استراتيجية

---

4. جهات الاتصال الطارئة / Emergency Contacts

الجهات الداخلية / Internal Contacts

المنصب / Position	الاسم / Name	الهاتف / Phone	البريد الإلكتروني / Email
الرئيس التنفيذي / CEO			
مدير تقنية المعلومات / CTO			
مدير أمن المعلومات / CISO			
المدير القانوني / Legal Director			

الجهات الخارجية / External Contacts

الجهة / Organization	جهة الاتصال / Contact	الهاتف / Phone	البريد الإلكتروني / Email
الشرطة / Police		999	
الدفاع المدني / Civil Defense		998	
هيئة الاتصالات / CITC			
المركز الوطني للأمن السيبراني / NCSC			

---

5. التوقيعات والاعتمادات / Signatures and Approvals

إعداد المصفوفة / Matrix Preparation

معد المصفوفة / Prepared by: - الاسم / Name: __ - *المنصب / Position:* __ - التوقيع / Signature: __ - *التاريخ / Date:* __

اعتماد المصفوفة / Matrix Approval

معتمد المصفوفة / Approved by: - الاسم / Name: __ - *المنصب / Position:* __ - التوقيع / Signature: __ - *التاريخ / Date:* __

تاريخ المراجعة التالية / Next Review Date

تاريخ المراجعة المقررة / Scheduled Review Date: ___

ملاحظات / Notes:
