نموذج الإبلاغ عن الحادث السيبراني

Cybersecurity Incident Report Form

معلومات أساسية / Basic Information

تاريخ الحادث / Incident Date: __
وقت الحادث / Incident Time: __
تاريخ الاكتشاف / Discovery Date: __
وقت الاكتشاف / Discovery Time: __

المبلغ / Reporter:
- الاسم / Name: __ - *المنصب / Position:* __ - القسم / Department: __ - *البريد الإلكتروني / Email:* __ - رقم الهاتف / Phone: ___

تصنيف الحادث / Incident Classification

نوع الحادث / Incident Type: - [ ] برمجيات خبيثة / Malware - [ ] اختراق الشبكة / Network Intrusion - [ ] تسريب البيانات / Data Breach - [ ] هجوم الحرمان من الخدمة / DoS/DDoS Attack - [ ] هندسة اجتماعية / Social Engineering - [ ] تصيد إلكتروني / Phishing - [ ] فقدان/سرقة الأجهزة / Device Loss/Theft - [ ] انتهاك السياسات / Policy Violation - [ ] أخرى / Other: ___

مستوى الخطورة / Severity Level: - [ ] منخفض / Low - [ ] متوسط / Medium - [ ] عالي / High - [ ] حرج / Critical

مستوى التأثير / Impact Level: - [ ] محدود / Limited - [ ] متوسط / Moderate - [ ] كبير / Significant - [ ] شديد / Severe

وصف الحادث / Incident Description

ملخص الحادث / Incident Summary:

الأنظمة المتأثرة / Affected Systems: - [ ] الخوادم / Servers - [ ] محطات العمل / Workstations - [ ] الشبكة / Network - [ ] التطبيقات / Applications - [ ] قواعد البيانات / Databases - [ ] البريد الإلكتروني / Email - [ ] المواقع الإلكترونية / Websites - [ ] الأنظمة السحابية / Cloud Systems

تفاصيل الأنظمة المتأثرة / Affected Systems Details:

البيانات المتأثرة / Affected Data: - [ ] بيانات شخصية / Personal Data - [ ] بيانات مالية / Financial Data - [ ] بيانات طبية / Medical Data - [ ] معلومات سرية / Confidential Information - [ ] ملكية فكرية / Intellectual Property - [ ] أخرى / Other: ___

عدد السجلات المتأثرة / Number of Affected Records: ___

التفاصيل التقنية / Technical Details

عناوين IP المشبوهة / Suspicious IP Addresses:

أسماء الملفات المشبوهة / Suspicious File Names:

رسائل الخطأ / Error Messages:

المؤشرات الأمنية / Security Indicators:

الإجراءات المتخذة / Actions Taken

الإجراءات الفورية / Immediate Actions: - [ ] عزل الأنظمة المتأثرة / Isolated affected systems - [ ] تغيير كلمات المرور / Changed passwords - [ ] إيقاف الخدمات المتأثرة / Stopped affected services - [ ] حفظ الأدلة / Preserved evidence - [ ] إبلاغ الإدارة / Notified management - [ ] إبلاغ الجهات الخارجية / Notified external parties

تفاصيل الإجراءات / Action Details:

الأثر والأضرار / Impact and Damage

الأثر على العمليات / Operational Impact: [ ] توقف كامل / Complete shutdown - [ ] توقف جزئي / Partial shutdown - [ ] تباطؤ في الأداء / Performance degradation - [ ] لا يوجد أثر / No impact

التكلفة المقدرة / Estimated Cost: تكلفة الاستجابة / Response cost: __ - *تكلفة التوقف / Downtime cost:* __ - تكلفة الإصلاح / Recovery cost: __ - *التكلفة الإجمالية / Total cost:* __

الجهات المبلغة / Notification

الجهات الداخلية المبلغة / Internal Parties Notified: [ ] الإدارة العليا / Senior Management - [ ] قسم تقنية المعلومات / IT Department - [ ] قسم الأمن السيبراني / Cybersecurity Team - [ ] الشؤون القانونية / Legal Department - [ ] العلاقات العامة / Public Relations

الجهات الخارجية المبلغة / External Parties Notified: [ ] الجهات التنظيمية / Regulatory Bodies - [ ] الشرطة / Law Enforcement - [ ] شركات التأمين / Insurance Companies - [ ] العملاء / Customers - [ ] الشركاء / Partners

المتابعة / Follow-up

الدروس المستفادة / Lessons Learned:

التوصيات / Recommendations:

الإجراءات الوقائية المطلوبة / Required Preventive Actions:

التوقيعات / Signatures

المبلغ / Reporter: الاسم / Name: __ *التوقيع / Signature:* __ التاريخ / Date: ___

مدير الأمن السيبراني / Cybersecurity Manager: الاسم / Name: __ *التوقيع / Signature:* __ التاريخ / Date: ___

الإدارة العليا / Senior Management: الاسم / Name: __ *التوقيع / Signature:* __ التاريخ / Date: ___

ملاحظات إضافية / Additional Notes:

للاستخدام الداخلي فقط / For Internal Use Only رقم الحادث / Incident Number: __ *حالة الحادث / Incident Status:* __ تاريخ الإغلاق / Closure Date: ___