الدائرة: برنامج الحكومة الإلكترونية

1- معلومات اساسية عن الوظيفة
1.1 مسمى الوظيفــة: محقق حوادث الحاسوب
2.1 الادارة/ المديرية: برنامج الحكومة الإلكترونية
3.1 القسم/الشعبة: أمن المعلومات
4.1 مسمى وظيفة الرئيس المباشر: رئيس قسم البنية التحتية وامن المعلومات

3-غرض الوظيفة

- الاستجابة الأولية للحوادث والتحقيق فيها وحفظ الأدلة

4- المهام والواجبـــات :

- جمع الأدلة وتحليلها باستخدام الأدوات المتعارف عليها في مجال أمن المعلومات والمعتمدة قانونيا اوحسب المعايير العالمية.
- المحافظة على الأدلة حسب المعايير العالمية.
- تنفيذ التحقيقات الرقمية على مستوى أجهزة المستخدمين في بيئة ميكروسوفت بشكل أساسي و نظم تشغيل أخرى.
- مهارة استخدام أدوات المراقبة الالكترونية في بيئة العمل المؤسسية.
- المعرفة بـ Microsoft Network infrastructure
- المعرفة بـ TCP/IP
- مهارة التواصل مع الإدارة غير الفنية وكتابة تقارير إدارية عن نتائج التحقيقات.
- كتابة التقارير الفنية عن نتائج التحقيقات
- كتابة سياسات وعمليات الاستجابة لحوادث أمن المعلومات
- تدريب فريق الاستجابة لحوادث أمن المعلومات.
- مراجعة ضوابط وإجراءات أمن المعلومات والمراقبة والتوصية بإجراءات التحسين.
- التعاون مع الجهات الوطنية و العالمية للتحقيق في حوادث و جرائم أمن المعلومات.
- العمل مع الفريق.
- المعرفة بالقوانين الوطنية افلمتعلقة بأمن المعلومات
- مهارة التعامل مع أنظمة جمع وتحليل سجلات أحداث أنظمة الشبكة المختلفة: مثل SIEM.

المتطلبات الاساسية والاضافية لاشغال الوظيفة

- **المؤهل العلمي والخبرات:**
- شهادة البكالوريوس في تكنولوجيا المعلومات أو في أي من الحقول العلمية ذات العلاقة.
- خبرة خمس سنوات على الاقل في مجالي التحقيقات الرقمية والاستجابة لحوادث أمن المعلومات

- **2.7 التدريب:**
  - شهادة تخصص في مجال التحقيقات الرقمية
  - CEH certified

- **3.7 المعارف والمهارات والقدرات:**
  - معرفة جيدة أو/و خبرة في أمن تكنولوجيا المعلومات في القطاع الحكومي والتجاري.
  - معرفة بآخر المستجدات في القضايا الأمنية الخاصة بتكنولوجيا المعلومات.
  - معرفة بالمعايير الدولية لأمن المعلومات مثل ISO 27001.
  - معرفة بالمعايير الدولية PKI و PCI.
  - فهم عميق للمخرجات الأمنية، و أدواتها، و نظم الشبكات، و أمن الإنترنت .
  - فهم عميق لبيئة العمل من النواحي الأمنية و الفيزيائية، و أنظمة الرقابة على وسائل النفاذ للشبكات.
  - فهم عميق لمبادئ تقييم المخاطر و كذلك لمبادئ إدارة المخاطر، طرق مراجعة التدقيق، و طرق تنفيذ السياسات و الرقابة عليها.
  - فهم جيد بأساليب إدارة الهوية الرقمية، و التوثيق، و تكنولوجيا التشفير .
  - مهارات ممتازة في الاتصال الكتابي والشفهي وباللغتين العربية والانجليزية.
  - مهارة عالية في الاتصالات الكتابية و الشفهية و باللغتين العربية و الإنجليزية

8- الاعتمادات:

جهة الاعتماد	الاسم	مسمى الوظيفة	التوقيع	التاريخ
1.8 **الدائرة المعنية**				
2.8 ديوان الخدمة المدنية				