المعلومات الأساسية			
معلومات أساسية عن الوظيفة 1.1			
تصنيف الوظيفة	الوظائف التخصصية		
المسمى الوظيفي	ضابط امن سيبراني	نوع الوظيفة	عقد محدد المدة بدوام كامل 121
الدائرة	مديرية أنظمة المعلومات	الفئة الوظيفية	الأولى
رتبة الوحدة التنظيمية	مديرية	المجموعة الوظيفية	الوظائف الرقمية وتكنولوجيا المعلومات والاتصال والامن
اسم الوحدة التنظيمية	مديرية أنظمة المعلومات	المستوى	الثاني او الثالث
مسمى وظيفة الرئيس المباشر	رئيس قسم الامن السيبراني وإدارة المعلومات وتحليل البيانات	المسمى القياسي الدال	فني تكنولوجيا معلومات انتخابية
رمز الوظيفة	121224200500	مسمى الوظيفة الفعلي	
حجم الموارد البشرية *		حجم موازنة الدائرة *	
تعبأ لشاغلي وظائف المجموعة الثانية من الفئة العليا *			
1.2 موقع الوظيفة في الهيكل التنظيمي للدائرة			
	امين عام الهيئة المستقلة للانتخاب		
	⌄		
	مدير انظمة المعلومات		
	⌄		
	⌄		
2. الغرض من الوظيفة			
المهمة الرئيسية للوظيفة (الهدف من الوظيفة)			
المساهمة في حماية أنظمة المعلومات والبنية التحتية الرقمية للهيئة من التهديدات والهجمات السيبرانية، وضمان تطبيق السياسات والإجراءات الأمنية، ومراقبة أمن الشبكات والأنظمة، وتحليل البيانات ذات الصلة بالأمن السيبراني بما يدعم استمرارية الأعمال وسلامة البرامج والانظمة في الهيئة.			
3. المهام والواجبات والمسؤوليات الرئيسية			
1.3 المهام التفصيلية والمسؤوليات			
مراقبة وتحليل أمن الأنظمة والشبكات باستخدام أنظمة كشف ومنع التهديدات (IDS/IPS) وأدوات المراقبة الأمنية			
متابعة تنبيهات نظام إدارة معلومات الأحداث الأمنية (SIEM) والتعامل مع الحوادث الأمنية وتحليلها والتوصية بالإجراءات التصحيحية			
تنفيذ اختبارات الاختراق والفحوصات الأمنية الدورية لتقييم نقاط الضعف في الأنظمة والشبكات			
المساهمة في إعداد خطط الاستجابة للحوادث (Incident Response Plans) وتنفيذها عند الحاجة			
إعداد تقارير فنية دورية حول حالة أمن المعلومات والحوادث المكتشفة والإجراءات المتخذة			
المشاركة في توعية وتدريب الموظفين على ضوابط ومعايير الأمن السيبراني			
دعم أنشطة التدقيق الداخلي والخارجي على نظام إدارة أمن المعلومات والمشاركة في إجراءات التحسين المستمر			
المساهمة في تنفيذ متطلبات الامتثال للمعايير الوطنية والدولية في مجال الأمن السيبراني وحماية البيانات			
إدارة ومراجعة صلاحيات الوصول للمستخدمين بانتظام، وضمان منح الصلاحيات وفق مبدأ أقل امتياز ممكن (Least Privilege) ومبدأ فصل المهام (Segregation of Duties)، بما يتوافق مع ضوابط التحكم بالوصول في نظام إدارة أمن المعلومات (ISMS)			
التعاون مع فرق إدارة البيانات لتحليل المعلومات المتعلقة بالحوادث الأمنية والأنماط السلوكية للهجمات			
دعم عمليات التحقق وسلامة وأمن البيانات الانتخابية أثناء مراحل العملية الانتخابية			
يتعاون مع الوحدات التنظيمة الاخرى لضمان عمليات امنية متماسكة .			
يساهم في تطوير وتحديث قواعد اكتشاف الاختراق الامني لنظام ا لمراقبة المركزي (SIEM) وإجراءات التشغيل القياسية (SOPs) لتحسين المراقبة الامنية.			
يشارك في اليات واجراءات العمل لضمان ادامه الجاهزية الدائمة لاكتشاف وإدارة حوادث الامن السيبراني			

4. مكونات الوظيفة

1.4 اتصالات العمل

الغرض من الاتصال	الأشخاص الذين يتم التواصل معهم	التكرار
ادارة العلاقات	الجمهور, الهيئات الدولية, الهيئات المحلية, زملاء العمل المباشرين, موظفي الدوائر الحكومية الاخرى, موظفين الوحدات الأخرى الوزارة/المؤسسة	يومي
تبادل معلومات روتينية متصلة بالعمل مباشرة	زملاء العمل المباشرين, موظفين الوحدات الأخرى الوزارة/المؤسسة	يومي
تنسيق العمل	زملاء العمل المباشرين, موظفي الدوائر الحكومية الاخرى, موظفين الوحدات الأخرى الوزارة/المؤسسة	أسبوعي
توضيح أساليب العمل وطرقه أو تفسير البرامج والأعمال	الهيئات المحلية, زملاء العمل المباشرين, موظفي الدوائر الحكومية الاخرى, موظفين الوحدات الأخرى الوزارة/المؤسسة	أسبوعي
عرض خطط عمل جديدة أو معدلة	زملاء العمل المباشرين, موظفي الدوائر الحكومية الاخرى, موظفين الوحدات الأخرى الوزارة/المؤسسة	ربع سنوي أو عند الحاجة

4.2 المتطلبات الذهنية لحل مشكلات العمل

المتطلبات الذهنية	المستوى المطلوب
القدرة على تحليل التهديدات السيبرانية وتحديد أسبابها	عالي
التفكير المنطقي والاستنتاجي لاتخاذ قرارات سريعة في المواقف الطارئة	عالي
القدرة على تقييم المخاطر ووضع خطط معالجة مناسبة	عالي
القدرة على فهم وتحليل البيانات المعقدة لاستخراج مؤشرات أمنية	عالي
التنبؤ بالمشكلات الفنية قبل وقوعها ووضع إجراءات وقائية	عالي

4.3 مجال العمل وتأثيره

حماية البنية التحتية الرقمية للهيئة وضمان سرية وسلامة البيانات الخاصة بالهيئة وكذلك العمليات الانتخابية، بما يعزز إجراءات سير العمل في الهيئة وكذلك ينعكس على نزاهة العملية الانتخابية ويحافظ على الثقة بالعملية الانتخابية، من خلال الوقاية من التهديدات السيبرانية والاستجابة السريعة لها

4.3.1 الصعوبة والتعقيد

تتسم الوظيفة بدرجة عالية من التعقيد نظرًا لتعاملها مع أنظمة انتخابية حساسة تتطلب حماية مستمرة على مدار الساعة، والتعامل مع تهديدات سيبرانية متطورة ومتغيرة باستمرار، حيث تشمل المهام تحليل الهجمات الإلكترونية المعقدة، وإدارة أنظمة الحماية المتقدمة، وضمان توازن دقيق بين متطلبات الأمن واحتياجات سهولة الاستخدام للأنظمة، كما تتطلب العمل تحت ضغط زمني مرتفع خاصة خلال فترة الانتخابات، واتخاذ قرارات فورية دقيقة لتفادي أي تأثير على نزاهة وسلامة سير العملية الانتخابية.

المسمى الوظيفي للمرؤوسين	درجة الوظيفة	عدد الموظفين

4.5 المجهود البدني وظروف العمل

4.5.1 المجهود البدني

مستوى ونوعية المجهود	% من وقت العمل
العمل المكتبي باستخدام الحاسوب ومتابعة الأنظمة الخاصة بمراقبة الأنظمة وتحليل البيانات وإعداد التقارير الفنية	85%
التعامل مع تجهيز وتركيب أو صيانة أجهزة ومعدات تقنية وشبكية والتنقل داخل الهيئة لمتابعة أعمال المراقبة أو الفحص	15%

4.5.2 ظروف العمل

مستوى ونوعية المجهود	مدى الشدة	% من وقت العمل
بيئة مكتبية مزودة بأجهزة الحاسوب والشبكات والأنظمة اللازمة		85%
العمل تحت ضغط مرتفع خلا ل مراحل التحضير للعملية الانتخابية		15%

5. المؤهلات العلمية والخبرات العملية	
1.5 متطلبات اشغال الوظيفة (الحد الأدنى من المؤهلات العلمية والخبرات العملية والتدريب)	
5.1.1 المؤهل العلمي المطلوب (الحد الأدنى)	
بكالوريس	
5.1.2 التخصص	
امن سيبراني،امن الشبكات ،امن المعلومات	
5.1.3 التدريب الفني او الإداري او التخصصي المطلوب (ويقصد التدريب الرسمي اللازم لممارسة عمل او مهنة معينة قبل شغل الوظيفة)	
الخبرة العملية المطلوبة	
نوع الخبرة العملية ومجالها	مدة الخبرة العملية / حد ادنى
الامن السيبراني وامن المعلومات وامن الشبكات	من دون خبرة
التدريب الفني او الإداري او التخصص المطلوب	
مستوى التدريب ومجاله	مدة التدريب
أساسيات أمن المعلومات والشبكات (Network & Information Security Fundamentals)	120 ساعة
أنظمة كشف ومنع الاختراق (IDS/IPS) وأنظمة المراقبة الأمنية (SIEM)	
5.2 الكفايات الوظيفية	
الكفايات السلوكية	
نوع الكفاية	مستوى الكفاية
التفكير التحليلي وحل المشكلات	متوسط
الدقة والانتباه للتفاصيل	متوسط
العمل تحت الضغط	متوسط
التواصل الفعال والعمل الجماعي	متوسط
التعلم المستمر ومواكبة التطورات التقنية	متوسط
إدارة الوقت وتنظيم العمل	متوسط
الالتزام بالسرية	متوسط
المبادرة واتخاذ القرار	متوسط
الالتزام بالأنظمة والتعليمات	متوسط
التفكير الاستراتيجي في إدارة المخاطر	متوسط
المرونة والتكيف مع التغيرات	متوسط
الكفايات الفنية	
نوع الكفاية	مستوى الكفاية
معرفة أمن الشبكات وأنظمة الحماية	متوسط
إدارة نظم الحماية الإلكترونية (Firewalls, IDS/IPS)	متوسط
تحليل التهديدات السيبرانية والاستجابة لها	متوسط
التعامل مع برامج مكافحة الفيروسات والبرمجيات الخبيثة	متوسط
تقييم واختبار اختراق الأنظمة (Penetration Testing)	متوسط
استخدام أدوات المراقبة وتحليل السجلات (SIEM)	متوسط
تطوير وتنفيذ سياسات أمن المعلومات	متوسط
فهم معايير وأطر العمل في الأمن السيبراني (ISO 27001)	متوسط

6. الموافقات			
الأدوار	المسمى الوظيفي	الاسم	التاريخ
الاعداد			
المراجعة			
الاعتماد			