إعلان توظيف

تعلن شركة حكومية وبالتنسيق مع هيئة الخدمة والادارة العامة عن حاجتها للوظائف التالية :

الوظيفة رقم (1)	المؤهلات العلمية المطلوبة	المؤهلات الفنية والخبرات المطلوبة
موظف أمن سيبراني خبرة	• درجة البكالوريوس كحد أدني في مجال الأمن السيبراني، أو أمن الشبكات أو أمن المعلومات أو هندسة الحاسوب أو علم الحاسوب أو أي تخصص له علاقة بطبيعة العمل، بتقدير لا يقل عن جيد. • يفضل أن يكون لديه شهادات مهنية مثل: – ISO 27001 lead implementer – شهادة أخصائي أمن نظم المعلومات المعتمد (CISSP) – Security+ – أخصائي الأمن السيبراني الصناعي GICSP	• خبرة لا تقل عن 3 سنوات في مجالات الأمن السيبراني أو أمن المعلومات. • فهم عميق لمجالات الأمن السيبراني وتقنياته المتقدمة وأدواته الحديثة في بيئة عمل تكنولوجيا المعلومات والتشغيل IT & OT. • الإلمام بالأدوات المستخدمة لمراقبة وحماية أنظمة تكنولوجيا المعلومات والتشغيل. • فهم البنية التحتية لتكنولوجيا المعلومات والتشغيل، بما في ذلك أنظمة التحكم والشبكات. • القدرة على تحليل المخاطر الأمنية ببيئة عمل تكنولوجيا المعلومات والتشغيل. • معرفة بمعايير الأمن السيبراني وأمن المعلومات الدولية والمحلية ذات الصلة ببيئات IT وOT، مثل ISO 27001، NIST CSF، ISA/IEC 62443 وغيرها. • معرفة في تحليل وتقييم الثغرات الأمنية. • مهارات الاستجابة الفعالة وإدارة الحوادث الأمنية وتتبعها. • القدرة على جمع وتحليل المعلومات حول التهديدات السيبرانية المحتملة وتحليل التنبيهات.

الوظيفة رقم (2)	المؤهلات العلمية المطلوبة	المؤهلات الفنية والخبرات المطلوبة
موظف أمن سيبراني حديث تخرج	• درجة البكالوريوس كحد أدني في مجال الأمن السيبراني، أو أمن الشبكات أو أمن المعلومات أو هندسة الحاسوب أو علم الحاسوب أو أي تخصص له علاقة بطبيعة العمل، بتقدير لا يقل عن جيد.	• فهم لمجالات الأمن السيبراني وتقنياته المتقدمة وأدواته الحديثة في بيئة عمل تكنولوجيا المعلومات والتشغيل IT & OT. • الإلمام بالأدوات المستخدمة لمراقبة وحماية أنظمة تكنولوجيا المعلومات والتشغيل. • القدرة على جمع وتحليل المعلومات حول التهديدات السيبرانية المحتملة وتحليل التنبيهات. • فهم اساسيات البنية التحتية لتكنولوجيا المعلومات ، بما في ذلك أنظمة التشغيل والشبكات.

الوظيفة رقم (3)	المؤهلات العلمية المطلوبة	المؤهلات الفنية	المهام الرئيسية المطلوبة
رئيس قسم وحدة الأمن السيبراني	• درجة البكالوريوس كحد أدني في مجال الأمن السيبراني، أو أمن الشبكات أو أمن المعلومات أو هندسة الحاسوب أو علم الحاسوب أو أي تخصص له علاقة بطبيعة العمل، بتقدير لا يقل عن جيد. • يفضل أن يكون لديه شهادات مهنية مثل: - ISO 27001 lead implementer - شهادة مدير أمن المعلومات المعتمد (CISM) - شهادة أخصائي أمن نظم المعلومات المعتمد (CISSP)	• خبرة عملية لا تقل عن 10 سنوات منها 3 سنوات على الاقل في مجالات الأمن السيبراني وكما يلي: 1- حماية الشبكات التشغيلية أو حماية البنى التحتية الحرجة. 2- ادارة المخاطر والقدرة على تحليل وإدارة المخاطر السيبرانية ببيئة عمل تكنولوجيا المعلومات والتشغيل OT/IT. 3- خبرة في تطبيق أطر عمل ومعايير الأمن السيبراني الدولية والمحلية ذات الصلة ببيئات IT وOT، مثل ISO 27001، NIST CSF، ISA/IEC 62443 وغيرها. 4- خبرة في صياغة وتطبيق السياسات والإجراءات الأمنية. • القدرة على وضع وتوجيه الاستراتيجيات الأمنية الشاملة التي تتماشى مع الأهداف التنظيمية، وتطوير خارطة طريق واضحة لتعزيز القدرات الأمنية للشركة. • مهارات قيادية وإدارية مع القدرة على بناء وتدريب وتوجيه فريق الأمن السيبراني. • القدرة على التواصل الفعال مع الإدارة العليا والجهات المعنية غير التقنية لشرح المخاطر الأمنية وتقديم الحلول الاستراتيجية. • فهم عميق لمختلف مجالات الأمن السيبراني وتقنياته المتقدمة وأدواته الحديثة.	• بناء الاستراتيجيات الخاصة بالأمن السيبراني، ووضع خطط تنفيذية لها. • وضع السياسات والتعليمات للأمن السيبراني ومتابعة تطبيقها. • التأكد من الامتثال للتشريعات والأنظمة والاستراتيجيات والمعايير والقوانين الوطنية المتعلقة بالأمن السيبراني. • دمج ممارسات الأمن السيبراني في جميع جوانب إدارة العمليات بالشركة، مثل حماية البيانات والموارد البشرية والأمن المادي ومشاريع الشركة أو الخدمات التي يتم شراؤها وغيرها. • إدارة المخاطر المتعلقة بالأمن السيبراني بكافة عمليات ومشاريع الشركة. • تقييم مستوى الأمن السيبراني بشكل مستمر ورفع التقارير والتوصيات بخصوصها للإدارة. • التحقق من توافق تصميم شبكة وأنظمة تكنولوجيا المعلومات وشبكات التشغيل والتحقق مع معايير الأمن السيبراني. • اجراء الفحوصات اللازمة مثل فحوصات الاختراق (Penetration Test) وفحوصات الثغرات (Vulnerability Scan) وغيرها. • تحديد المتطلبات التقنية اللازمة لتحقيق مستوى أمن سيبراني مناسب بالشركة، والمساهمة في دراسة وتحديد متطلبات الأمن السيبراني الملائمة عند شراء أو بناء أنظمة المعلومات بالشركة أو أنظمة التشغيل أو البنية التحتية المتعلقة بها. • توعية الموظفين حول الأمن السيبراني. • مراقبة شبكة تكنولوجيا المعلومات وشبكات التشغيل. • الاستجابة للحوادث الأمنية ووضع خطة للتعامل معها.

الشروط العامة للوظائف اعلاه:

1. أن يكون المتقدم اردني الجنسية وأن يكون لائق صحياً وغير محكوم بأي جناية او جنحه.
2. أن لا يزيد عمر المتقدم عن (30) سنة لوظيفة رقم (1 ، 2) وعن (45) سنة لوظيفة رقم (3).
3. يتم إعتماد التخصص حسب المصدقة الجامعية للبكالوريوس.
4. أن يقبل العمل في أي موقع من مواقع عمل الشركة.
5. يستبعد اي طلب يتبين انه يتضمن معلومات غير صحيحة.

الوثائق المطلوب إرفاقها مع الطلب:

1. صورة مصدقة عن الشهادة الجامعية البكالوريوس لوظيفة (رئيس قسم و موظف الأمن السيبراني) .
2. صورة عن شهادة انتساب لعضوية نقابة المهندسين سارية المفعول في حال كانت الشهادة بكالوريوس في الهندسة.
3. صورة مصدقة عن كشف علامات الشهادة الثانوية العامة .
4. صورة عن وجهي البطاقة الشخصية الصادرة عن دائرة الأحوال المدنية .

على من تتوفر فيه الشروط السابقة ولديه الرغبة تقديم طلب على رابط هيئة الخدمة والادارة العامة التالي : https://applyjobs.spac.gov.jo

وذلك اعتباراً من تاريخ 2025/11/30 ولغاية نهاية يوم 2025/12/04 .

علماً بأنه لن يتم النظر في أي طلب لا تتوفر فيه الشروط أعلاه أو ورد قبل أو بعد فترة الإعلان أو غير معزز بالوثائق المطلوبة كاملة أو لم يحدد فيه رقم الوظيفة المطلوبة .