

 أدوار ومسؤوليات الأمن السيبراني

|  |
| --- |
|  |
|  |
|  |
|  |  |

**مدير إدارة الأمن السيبراني**

| # | المسؤوليات |
| --- | --- |
|  | الإشراف على تطوير استراتيجية الأمن السيبراني وتحديثها. |
|  | الإشراف على تطوير وتنفيذ منهجيات وإجراءات مراقبة حوادث الأمن السيبراني، وتوجيه أنشطة الأمن السيبراني ومتابعتها بشكل مستمر ورفع التقارير الخاصة بها. |
|  | الإشراف على تطوير وتحديث منهجية وإجراءات إدارة مخاطر الأمن السيبراني. |
|  | التأكد من تطوير معايير وإجراءات الأمن السيبراني والموافقة عليها وتطبيقها. |
|  | الإشراف على تطوير سياسات الأمن السيبراني وتحديثها بناءً على متطلبات الأمن السيبراني. |
|  | التأكّد من توافق إدارة مخاطر الأمن السيبراني مع إدارة المخاطر في جامعة الإمام محمد بن سعود الإسلامية. |
|  | تقديم حلول وتوصيات حول الأمن السيبراني لتقليل المخاطر السيبرانية على الأصول المعلوماتية والتقنية.  |
|  | تقديم التوجيهات والدعم اللازم ومعالجة المسائل المتعلقة بتخطيط وإدارة الموارد البشرية الخاصة بالأمن السيبراني (مثل: التوظيف والاحتفاظ بالموظفين والتدريب). |
|  | الإشراف على تحديد متطلبات الأمن السيبراني وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة والتأكد من الالتزام بها. |
|  | الإشراف على حوادث الاستجابة للأمن السيبراني ورفع التقارير الخاصة بها. |
|  | الإشراف على التقييم المستمر للثغرات ومتابعة تطبيق حزم التحديثات الأمنية والإعدادات. |
|  | الإشراف على جمع وتحليل المعلومات الاستباقية المتعلقة بالأمن السيبراني من المصادر الوطنية أو المصادر الدولية. |
|  | الإشراف على إجراء اختبارات اختراق دورية على جميع الخدمات المقدمة خارجياً ومكوناتها التقنية لتقييم مستوى الأمن السيبراني. |
|  | الإشراف على إعداد مبادئ تصميم الأمن السيبراني، وتصاميم الأمن السيبراني للأنظمة والشبكات، ومعمارية الأمن السيبراني، مع ضمان المواءمة مع المعمارية المؤسسيةEnterprise) Architecture). |
|  | الإشراف على إدارة الوصول المنطقي (Logical Access) إلى الأصول المعلوماتية والتقنية لجامعة الأمام محمد بن سعود الإسلامية من خلال تحديد متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات في جامعة الإمام محمد بن سعود الإسلامية وتوثيقها وتطبيقها. |
|  | الإشراف على إعداد الميزانية الخاصة بتنفيذ مبادرات ومشاريع الأمن السيبراني. |
|  | التأكد من مراجعة متطلبات الأمن السيبراني دورياً. |
|  | توفير الدعم والإشراف على إعداد آلية مناسبة لقياس مؤشرات الأداء (KPIs) لأعمال الأمن السيبراني ومشاركتها مع اللجنة الإشرافية للأمن السيبراني. |
|  | التواصل مع الهيئة الوطنية للأمن السيبراني وإدارة العلاقة معها. |
|  | الإشراف على برامج الأمن السيبراني ومنها برنامج التوعية بالأمن السيبراني. |

**موظفو إدارة الأمن السيبراني**

| # | المسؤوليات |
| --- | --- |
|  | تطوير سياسات وإجراءات ومعايير الأمن السيبراني ومراجعتها سنوياً. |
|  | تحديد منهجية وإجراءات إدارة مخاطر الأمن السيبراني وتطبيقها ومراجعتها دورياً. |
|  | الـتأكد من تطبيق سياسات وإجراءات ومعايير الأمن السيبراني. |
|  | تطبيق عملية إدارة مخاطر الأمن السيبراني وتنفيذها. |
|  | إجراء تقييمات المخاطر، ومتابعة وضع المخاطر والإجراءات التي تم اتخاذها بالتنسيق مع أصحاب المصلحة. |
|  | تحديد المسؤوليات المتعلقة بالمخاطر بالتنسيق مع أصحاب المصلحة. |
|  | إعداد تقارير تقييم المخاطر واعتمادها من قبل مدير إدارة الأمن السيبراني. |
|  | تنفيذ برنامج الالتزام بالأمن السيبراني ومراجعته سنوياً. |
|  | تطوير برنامج التوعية والتدريب بالأمن السيبراني. |
|  | تطبيق برنامج التوعية والتدريب بالأمن السيبراني بالتنسيق مع عميد عمادة الموارد البشرية وقياس مدى التزام العاملين بالتوعية بالأمن السيبراني. |
|  | إعداد تقارير الالتزام بمتطلبات الأمن السيبراني واعتمادها من قبل إدارة الأمن السيبراني. |
|  | القيام بأنشطة المراقبة وإعداد التقارير المتعلقة بالالتزام بالأمن السيبراني. |
|  | توفير نظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني (SIEM) ومراقبته. |
|  | متابعة أنظمة مراقبة الأمن السيبراني للتأكد من استقرارها وتوافرها، وتقديم تقارير لوصف حالتها. |
|  | جمع أحداث الأمن السيبراني في الأصول المعلوماتية والتقنية في نظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني (SIEM)، وتحليل السجلات، وتحديد مخاطر الأمن السيبراني. |
|  | التعامل مع حوادث الأمن السيبراني ومتابعة إغلاقها، وتصعيد الأحداث القائمة التي تتجاوز اتفاقية مستوى الخدمة المحددة. |
|  | التقييم المستمر للثغرات ومتابعة تطبيق حزم التحديثات الأمنية والإعدادات. |
|  | إجراء اختبارات اختراق دورية على جميع الخدمات المقدمة خارجياً ومكوناتها التقنية لتقييم مستوى الأمن السيبراني. |
|  | إعداد مبادئ تصميم الأمن السيبراني وتصاميم الأمن السيبراني للأنظمة والشبكات ومعمارية الأمن السيبراني، مع ضمان المواءمة مع المعمارية المؤسسية (Enterprise Architecture). |
|  | إدارة الوصول المنطقي (Logical Access) إلى الأصول المعلوماتية والتقنية لجامعة الإمام محمد بن سعود الإسلامية من خلال تحديد متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات في جامعة الإمام محمد بن سعود الإسلامية وتوثيقها وتطبيقها. |