الموضوع: تعميم بشأن ضوابط وسياسات الأمن السيبراني.

# الضوابط والسياسات للأمن السيبراني بالجامعة

- **البنود العامة:**

١-١ يجب التعامل مع المعلومات حسب التصنيف المحدد، وبما يتوافق مع سياسة تصنيف البيانات وسياسة حماية البيانات والمعلومات الخاصة بجامعة الامام محمد بن سعود بشكل يضمن حماية سرية المعلومات وسلامتها وتوافرها.

١-٢ يحظر انتهاك حقوق أي شخص، أو شركة محمية بحقوق النشر، أو براءة الاختراع، أو أي ملكية فكرية أخرى أو قوانين أو لوائح مماثلة؛ بما في ذلك، على سبيل المثال لا الحصر، تثبيت برامج غير مصرح بها أو غير قانونية.

١-٣ يجب عدم ترك المطبوعات على الطابعة المشتركة دون رقابة.

١-٤ يجب حفظ وسائط التخزين الخارجية بشكل آمن وملائم.

١-٥ يمنع استخدام كلمة المرور الخاصة بمستخدمين آخرين، بما في ذلك كلمة المرور الخاصة بمدير المستخدم أو مرؤوسيه.

١-٦ يجب الالتزام بسياسة المكتب الآمن والنظيف، والتأكد من خلو سطح المكتب، وكذلك شاشة العرض من المعلومات المصنفة.

١-٧ يمنع الإفصاح عن أي معلومات تخص جامعة الامام محمد بن سعود، بما في ذلك المعلومات المتعلقة بالأنظمة والشبكات لأي جهة أو طرف غير مصرح له سواءً كان ذلك داخلياً أو خارجياً.

١-٨ يُمنع نشر معلومات تخص جامعة الامام محمد بن سعود عبر وسائل الإعلام، وشبكات التواصل الاجتماعي دون تصريح مسبق.

١-٩ يُمنع استخدام أنظمة جامعة الامام محمد بن سعود وأصولها بغرض تحقيق منفعة وأعمال شخصية، أو تحقيق أي غرض لا يتعلق بنشاط وأعمال جامعة الامام محمد بن سعود.

١-١٠ يُمنع ربط الأجهزة الشخصية بالشبكات، والأنظمة الخاصة بجامعة الامام محمد بن سعود دون الحصول على تصريح مسبق، وبما يتوافق مع سياسة أمن الأجهزة المحمولة (BYOD).

١-١١ يُمنع القيام بأي أنشطة تهدف إلى تجاوز أنظمة الحماية الخاصة بجامعة الامام محمد بن سعود، بما في ذلك برامج مكافحة الفيروسات، وجدار الحماية، والبرمجيات الضارة دون الحصول على تصريح مسبق، وبما يتوافق مع الإجراءات المعتمدة لدى جامعة الامام محمد بن سعود.

١-١٢ تحتفظ ادارة الامن السيبراني بحقها في مراقبة الأنظمة والشبكات والحسابات الشخصية المتعلقة بالعمل ومراجعتها دورياً لمراقبة الالتزام بسياسات الأمن السيبراني ومعاييره.

١-١٣ يُمنع استضافة أشخاص غير مصرح لهم بالدخول للأماكن الحساسة دون الحصول على تصريح مسبق.

١-١٤ يجب تبليغ ادارة الامن السيبراني في حال فقدان المعلومات أو سرقتها أو تسريبها.

الموضوع: تعميم بشأن ضوابط وسياسات الأمن السيبراني.

- **حماية أجهزة الحاسب:**

٢-١ يمنع استخدام وسائط التخزين الخارجية دون الحصول على تصريح مسبق من ادارة الامن السيبراني.

٢-٢ يُمنع القيام بأي نشاط من شأنه التأثير على كفاءة الأنظمة والأصول وسلامتها دون الحصول على إذن مسبق من ادارة الامن السيبراني، بما في ذلك الأنشطة التي تُمكّن المستخدم من الحصول على صلاحيات وامتيازات أعلى.

٢-٣ يجب تأمين الجهاز قبل مغادرة المكتب وذلك بقفل الشاشة، أو تسجيل الخروج (Sign out or Lock) سواء كانت المغادرة لفترة قصيرة أو عند انتهاء ساعات العمل.

٢-٤ يُمنع ترك أي معلومات مصنفة في أماكن يسهل الوصول إليها، أو الاطلاع عليها من قبل أشخاص غير مصرح لهم.

٢-٥ يُمنع تثبيت أدوات خارجية على جهاز الحاسب الآلي دون الحصول على إذن مسبق من إدارة الأمن السيبراني.

٢-٦ يجب تبليغ إدارة الأمن السيبراني عند الاشتباه بأي نشاط قد يتسبب بضرر على أجهزة الحاسب الآلي الخاصة بـ جامعة الامام محمد بن سعود أو أصولها.

- **الاستخدام المقبول من الأنترنت والبرمجيات:**

٣-١ يجب إبلاغ إدارة الأمن السيبراني في حال وجود مواقع مشبوهة ينبغي حجبها؛ أو العكس.

٣-٢ يجب ضمان عدم انتهاك حقوق الملكية الفكرية أثناء تنزيل معلومات أو مستندات لأغراض العمل.

٣-٣ يُمنع استخدام البرمجيات غير المرخصة أو غيرها من الممتلكات الفكرية.

٣-٤ يجب استخدام متصفح آمن ومصرح به للوصول إلى الشبكة الداخلية أو شبكة الإنترنت.

٣-٥ يُمنع استخدام التقنيات التي تسمح بتجاوز الوسيط (Proxy) أو جدار الحماية (Firewall) للوصول إلى شبكة الإنترنت.

٣-٦ يُمنع تنزيل البرمجيات والأدوات أو تثبيتها على أصول جامعة الامام محمد بن سعود دون الحصول على تصريح مسبق من إدارة الأمن السيبراني.

٣-٧ يُمنع استخدام شبكة الإنترنت في غير أغراض العمل، بما في ذلك تنزيل الوسائط والملفات واستخدام برمجيات مشاركة الملفات.

٣-٨ يجب تبليغ إدارة الأمن السيبراني عند الاشتباه بوجود مخاطر سيبرانية، كما يجب التعامل بحذر مع الرسائل الأمنية التي قد تظهر خلال تصفح شبكة الإنترنت أو الشبكات الداخلية.

٣-٩ يُمنع إجراء فحص أمني لغرض اكتشاف الثغرات الأمنية، ويشمل ذلك إجراء اختبار الاختراقات، أو مراقبة شبكات جامعة الامام محمد بن سعود وأنظمتها، أو الشبكات والأنظمة الخاصة بالجهات الخارجية دون الحصول على تصريح مسبق من إدارة الأمن السيبراني.

٣-١٠ يُمنع استخدام مواقع مشاركة الملفات دون الحصول على تصريح مسبق من إدارة الأمن السيبراني.

٣-١١ يُمنع زيارة المواقع المشبوهة بما في ذلك مواقع تعليم الاختراق.

- **الاستخدام المقبول للبريد الإلكتروني ونظام الاتصالات:**

٤-١ يُمنع استخدام البريد الإلكتروني أو الهاتف أو الفاكس أو الفاكس الإلكتروني في غير أغراض العمل، وبما يتوافق مع سياسات الأمن السيبراني ومعاييره.

٤-٢ يُمنع تداول رسائل تتضمن محتوى غير لائق أو غير مقبول، بما في ذلك الرسائل المتداولة مع الأطراف الداخلية والخارجية.



٤-٣ يجب استخدام تقنيات التشفير عند إرسال معلومات حساسة عن طريق البريد الإلكتروني أو أنظمة الاتصالات.

٤-٤ يجب عدم تسجيل عنوان البريد الإلكتروني الخاص بجامعة الامام محمد بن سعود في أي موقع ليس له علاقة بالعمل.

٤-٥ يجب تبليغ إدارة الأمن السيبراني عند الاشتباه بوجود رسائل بريد إلكتروني تتضمن محتوى قد يتسبب بأضرار لأنظمة جامعة الامام محمد بن سعود أو أصولها.

٤-٦ تحتفظ جامعة الامام محمد بن سعود بحقها في كشف محتويات رسائل البريد الإلكتروني بعد الحصول على التصاريح اللازمة من صاحب الصلاحية وإدارة الأمن السيبراني وفقاً للإجراءات والتنظيمات ذات العلاقة.

٤-٧ يُمنع فتح رسائل البريد الإلكتروني والمرفقات المشبوهة أو غير المتوقعة حتى وإن كانت تبدو من مصادر موثوقة.

- **الاجتماعات المرئية والاتصالات القائمة على شبكة الإنترنت:**



٥-١ يُمنع استخدام أدوات أو برمجيات غير مصرح بها لإجراء اتصالات أو عقد اجتماعات مرئية.

٥-٢ يُمنع إجراء اتصالات أو عقد اجتماعات مرئية لا تتعلق بالعمل دون الحصول على تصريح مسبق.

- **استخدام كلمات المرور:**

٦-١ يجب اختيار كلمات مرور آمنة، والمحافظة على كلمات المرور الخاصة بأنظمة جامعة الامام محمد بن سعود وأصولها. كما يجب اختيار كلمات مرور مختلفة عن كلمات مرور الحسابات الشخصية مثل حسابات البريد الشخصي ومواقع التواصل الاجتماعي.

٦-٢ يُمنع مشاركة كلمة المرور عبر أي وسيلة كانت، بما في ذلك المراسلات الإلكترونية، والاتصالات الصوتية، والكتابة الورقية. كما يجب على جميع المستخدمين عدم الكشف عن كلمة المرور لأي طرف آخر بما في ذلك زملاء العمل وموظفو عمادة تقنية المعلومات.



٦-٣ يجب تغيير كلمة المرور، عند تزويدك بكلمة مرور جديدة من قبل مسؤول النظام.