سياسة الاستخدام الآمن لتقنية المعلومات

رقم الوثيقة: IMSIU-IT-ISMS-POL-023

ـ وثيقة عامة ـ

ربيع الأول ١٤٣٥هـ

معلومات إدارة الوثيقة

عنوان الوثيقة: سياسة الاستخدام الآمن لتقنية المعلومات

حالة الوثيقة: معتمدة

تفاصيل الإصدار

تاريخ الإصدار	١٤٣٥/٤/٩ه الموافق ٢٠١٤/٢/٩م

تفاصيل جهات الإتصال الخاصة بالوثيقة

الدور	الإسم
المالك	عمادة تقنية المعلومات "إدارة أمن المعلومات "

قائمة التوزيع

الإسم
جميع موظفي ومنسوبي ومتعاقدي جامعة الإمام محمد بن سعود الإسلامية والفروع والمعاهد التابعة لها.

جدول المحتويات

سياسة الاستخدام الآمن لتقنية المعلومات

١. بيانات السياسة

تحدد هذه السياسة الحد الأدنى من متطلبات القواعد الأمنية الأخلاقية لمنسوبي جامعة الإمام محمد بن سعود الإسلامية والمتعاقدين والمقاولين ،و تتناول عزم جامعة الإمام محمد بن سعود الإسلامية في حماية أصول المعلومات و مصادر الحوسبة من التهديدات. كذلك تحدد هذه السياسة آداب الإستخدام الصحيح لأجهزة الحاسب الآلي، و الشبكة العنكبوتية (الإنترنت) و استخدام البريد الإلكتروني، و تحدد إجراءات الحماية من التهديدات المنقولة عبر الإنترنت و البريد الإلكتروني. و القصد من هذه السياسة أن تكون وثيقة يتم توزيعها على كافة منسوبي جامعة الإمام محمد بن سعود الإسلامية وفروعها والمعاهد التابعة لها .

٢. تفاصيل السياسة

تُطبق سياسة الاستخدام الآمن لتقنية المعلومات هذه على كل فرد ينضم إلى جامعة الإمام محمد بن سعود الإسلامية، وعليه، يجب على كل من منسوبي الجامعة التقيد سياسة الاستخدام الآمن لتقنية المعلومات ، حيث ستؤدي مخالفة سياسة الاستخدام الآمن لتقنية المعلومات هذه أو عدم التقيد بها إلى إتخاذ إجراء تأديبي.

المعايير الأمنية والأخلاقية

- **أخلاقيات العمل:** يجب على كل موظف، في كافة الأوقات، التصرف بنزاهة وأداء كافة المهام الموكلة إليه بما يتفق مع القوانين المطبقة في المملكة العربية السعودية و سياسات و إجراءات جامعة الإمام محمد بن سعود الإسلامية. وعلى كل موظف أداء واجباته بطريقة صادقة، وصريحة و شاملة.

- **السرية:** يجب على الموظفين الحفاظ على سرية المعلومات السرية الموكلة إليهم، وعدم الكشف عنها إلا للأشخاص المصرح لهم من قبل الموظف القانوني المناسب في جامعة الإمام محمد بن سعود الإسلامية. وتشمل المعلومات السرية كافة المعلومات غير العامة التي قد تكون ذات فائدة بالنسبة لمؤسسات أخرى أو ضارة بالنسبة لجامعة الإمام محمد بن سعود الإسلامية إذا تم الكشف عنها. كما تشمل أيضا المعلومات التي تعهد بها أطراف أخرى (كالمقاولين، أو الموردين أو الجهات الحكومية الأخرى) لجامعة الإمام محمد بن سعود الإسلامية. و يستمر الإلتزام بالحفاظ على المعلومات السرية حتى بعد إنتهاء التوظيف.
- **تضارب المصالح:** ينشأ تضارب المصالح عندما تتداخل المصلحة الشخصية لشخص ما، بأي طريقة، مع مصالح الجامعة, لذا يجب على الموظف عدم أداء أي مهام تنطوي على تضارب في المصالح.
- **التعامل العادل:** على الموظفين التصرف بصدق وأخلاق في كافة الأوقات ومع كافة الأشخاص. ولا ينبغي على أي شخص الإستفادة بشكل غير عادل من أي شخص من خلال التلاعب، أو الإخفاء، أو إساءة استخدام المعلومات السرية، أو تحريف الوقائع المادية، أو أي ممارسة أخرى غير عادلة.
- **حماية أصول الجامعة واستخدامها بالشكل الصحيح:** ينبغي على كافة الموظفين بذل الجهد لحماية أصول جامعة الإمام محمد بن سعود الإسلامية وضمان إستخدامها بشكل فعال. و سيكون لإفشاء السرية، و الإهمال و الهدر تأثير مباشر على أداء جامعة الإمام محمد بن سعود الإسلامية. وينبغي الإبلاغ فورا عن أي حالة لإفشاء السرية أو إنتهاك سياسة أمن المعلومات للتحقيق فيها. ولا يجوز استخدام موارد و معدات جامعة الإمام محمد بن سعود الإسلامية لأغراض بخلاف تلك

الخاصة بالجامعة، إلا أن الاستخدام الشخصي العرضي مسموح. و يجب على الموظفين التقيد بسياسةالاستخدام الآمن لتقنية المعلومات لجامعة الإمام محمد بن سعود الإسلامية.

- **الإبلاغ عن المخالفات:** ينبغي على الموظف إبلاغ مركز عمليات أمن المعلومات و المشرفين، و المدراء أو غيرهم من الموظفين المناسبين حول السلوك غير القانوني أو غير الآمن الذي يطلع عليه أو يشتبه به. ولن يُسمح بأي تصرف إنتقامي ضد أي شخص يقوم بأي عملية إبلاغ.

٣. توجيهات عامة

٣,١ أمن النظم و الشبكة

تعتبر مخالفات أمن النظام أو الشبكة محظورة تماما وقد تؤدي إلى مسئولية جزائية أو مدنية، مالم يتم التصريح بها. ويشمل ذلك (على سبيل المثال لا الحصر) التالي: الاستخدام غير المصرح به أو الصلاحيات، أو الفحص أو المسح لأمن الأنظمة أو إجراءات التوثيق للبيانات أو كلمات المرور؛ و التداخل مع صلاحيات خدمة أي مستخدم آخر،أو نظام أو شبكة (على سبيل المثال لا الحصر) البريد الإلكتروني الضار، أو الإغراق، أو المحاولات المتعمدة لتحميل نظام ما بشكل زائد عن الحد، أو تزوير عناوين الأجهزة (عناوين الإنترنت) أو البريد التطفلي, أو نشر البرامج الخبيثة.

٣,٢ وسائل التخزين

يتم استخدام أي وسيلة تخزين، على سبيل المثال لا الحصر الأقراص الضوئية (CD)، والأقراص المضغوطة، الأقراص القابلة للإزالة (Flash drive)، فقط بعد الحصول على الموافقة المسبقة من عمادة تقنية المعلومات. و يمنع منعا باتا استخدام الأجهزة الخلوية ذات الكاميرات في المناطق المؤمنة بشكل كبير مثل غرفة الخوادم.

٣,٣ البيانات غير القانونية

يمنع منعا باتا نقل، أو تخزين، أو توزيع أي معلومات، أو بيانات أو مواد تخالف القانون أو النظام المطبق. و يشمل ذلك، على سبيل المثال لا الحصر: بيانات الطلاب، و بيانات الموظفين، و بيانات المنافسات والتعاقد، أو أي ملكية فكرية أخرى تستخدم دون تصريح صحيح، والمواد المخلة بالآداب، أو المسيئة للسمعة أو تلك التي تشكل تهديدا غير مشروع.

٤. استخدام أجهزة الحاسب الآلي

٤,١ استخدام سطح المكتب

يكون الموظفين مسئولين عن أمن المعلومات المخزنة على أجهزة الحاسب المكتبي. وينبغي أن يدرك المستخدمون أن البيانات التي يقومون بإنشائها على أنظمة الشركة ستبقى ملكا لجامعة الإمام محمد بن سعود الإسلامية. وتشتمل مسئولية المستخدم على إنشاء نسخ إحتياطية على أقراص عادية، و التحكم بنفاذ الشبكة على الجهاز، واستخدام برمجيات الحماية من الفيروسات المعتمدة من الجامعة. و تشمل النسخ الإحتياطية أيضا النسخة الإحتياطية من السجل.

٤,٢ إغلاق أجهزة الحاسب الألي

ينبغي على مستخدمي جامعة الإمام محمد بن سعود الإسلامية تسجيل الخروج أو إغلاق اجهزة الحاسب الآلي أثناء تواجدهم في أماكن بعيدة عن مكاتبهم لأي فترة زمنية. و يتم ضبط أجهزة الحاسب الآلي على الإغلاق الإتوماتيكي باستخدام حافظة الشاشة الآمنة إذا لم يتم استخدامها لمدة أكثر من ٥ دقائق.

٤,٣ العمل الشخصي

لا يمكن استخدام أجهزة الحاسب الألي و الأنظمة و الخدمات و الشبكات لأعمال بخلاف تلك المطلوبة لتشغيل جامعة الإمام محمد بن سعود الإسلامية.

٤,٤ تبادل ومشاركة البيانات

لا يسمح بتبادل الملفات والبيانات إلا بالتصريح المسبق من عمادة تقنية المعلومات، ويتم الحصول على ذلك من خلال طلبه من عمادة تقنية المعلومات واتباع الاجراءات المطلوبة للحفاظ على أمن البيانات. ويُنصح بأن يتم تشفير أي معلومات يرى المستخدمون أنها حساسة أو ضعيفة خلال عملية النقل تلك. كما ينبغي تفادي تخزين كلمات السر أو المعلومات الأخرى التي يمكن استخدامها للحصول على الصلاحيات لمصادر الشبكة أو الأنظمة. ويتم إسناد حسابات الحاسب، وكلمات السر، و أنواع التصاريح الأخرى لموظفين أفراد مسئولين عن أمنها. ويُمنع منعا باتا الكشف عن كلمة المرور للحساب الشخصي لأطراف أخرى أو السماح باستخدام الحساب الشخصي من قبل آخرين.

٤,٥ استخدام الصلاحيات المميزة (Administration Privilege)

يتم استخدام النفاذ إلى المعلومات أو غيرها من إمتيازات الحوسبة الخاصة خلال العمل الرسمي فقط. ويتم التعامل مع المعلومات المتوفرة من خلال مزايا خاصة على أنها خاصة و سرية. وأي محاولة متعمدة لخفض أداء الأنظمة أو الشبكة أو الوصول لأي بنية تحتية محظورة لتقنية المعلومات تعتبر محظورة.

٤,٦ تراخيص البرمجيات

- يجب أن تحمل كافة البرمجيات التي يتم تركيبها على أجهزة الأفراد تراخيص سارية المفعول و صحيحة.

- لا ينبغي على المستخدمين نسخ البرمجيات من الشبكة وضعها أو تنصيبها على أي أجهزة دون الحصول على التراخيص المناسبة من عمادة تقنية المعلومات.
- لا يقوم المستخدمون بتوزيع البرمجيات إذا لم يكن لديهم الحق للقيام بذلك.

٤,٧ أنشطة الاستخدام غير المقبول

- يُمنع منعا باتا ممارسة الأنشطة الضارة كإنشاء الفيروسات أو نشرها؛ و تعطيل الخدمات؛ و إتلاف الملفات؛ أو إلحاق الضرر بالأنظمة، أو البرمجيات، أو التطبيقات، أو البيانات المتعلقة بجامعة الإمام محمد بن سعود الإسلامية.
- يُمنع بشكل صريح إجراء المسح الإلكتروني لمنافذ النظمة أو المسح الأمني للتطبيقات والأنظمة مالم يتم الحصول على تصريح صريح من مسؤول أمن المعلومات.
- يُمنع تنفيذ أي شكل من أشكال مراقبة الشبكة أو البيانات المخزنة أو المرسلة ، مالم يكن هذا النشاط ضمن نطاق المهام الوظيفية.
- يُمنع جمع معلومات عن الأنظمة عن طريق المسح الألكتروني أو أي طريقة بما في ذالك استخدام الأدوات والبرامج الخاصة باستقصاء معلومات عن الأنظمة.
- يُمنع تفعيل اختراقات أمنية أو إحداث أعطال بإتصالات الشبكة. حيث تشمل الإختراقات الأمنية، على سبيل المثال لا الحصر، إدخال بيانات لا يكون الموظف هو المتلقي المقصود بها أو الدخول على خادم أو حساب لا يصرح للموظف بشكل صريح الدخول إليه، مالم تكن تلك المهام ضمن نطاق المهام الوظيفية, و يشمل "التعطيل"، على سبيل المثال لا الحصر، مراقبة الشبكة، وإغراقها ، و محاولة إشغال الخدمة، وتزوير عناوين الاتصال.

٤,٨ الصلاحيات غير المصرح بها

على موظفي جامعة الإمام محمد بن سعود الإسلامية والفروع والمعاهد التابعة لها تفادي التالي:

- إلحاق الضرر بأنظمة الحاسب.
- الحصول على مصادر إضافية غير مصرح بها للفرد.
- حرمان مستخدم آخر من المصادر المصرح بها.
- الحصول على صلاحيات غير مصرح بها على الأنظمة.

وذلك عن طريق معرفة التالي:

- كلمة مرور خاصة.
- نقاط الضعف في أنظمة الحاسوب.
- كلمة المرور الخاصة بمستخدم آخر في جامعة الإمام محمد بن سعود الإسلامية.
- القدرة على الحصول على صلاحيات أعلى من المفترض لمستخدم في جامعة الإمام محمد بن سعود الإسلامية.

٥. استخدام الإنترنت

٥,١ تقييد الاستخدام بالعمل فقط

يتم استخدام الإنترنت فقط لأغراض العمل والدراسة والبحوث العلمية وما يتعلق في ذلك فقط.

٥,٢ تمثيل جامعة الإمام محمد بن سعود الإسلامية

يتم استخدام إتصالات الإنترنت فقط لأغراض العمل الصحيحة. و عليه، فإن أي معلومات يتم نشرها في مجموعات النقاش التي تحمل عنوان جامعة الإمام محمد بن سعود الإسلامية، ينبغي أن تمثل مواقف جامعة الإمام محمد بن سعود الإسلامية.

٥,٣ رسائل البريد الإلكتروني العامة

لا تعتبر أي رسالة يتم إرسالها عبر الإنترنت آمنة مالم يتم إتخاذ المزيد من التدابير لحماية المعلومات (على سبيل المثال، التشفير). و يقوم المستخدمون بالتواصل عبر البريد الإلكتروني كما يفعلون في الأماكن العامة (على سبيل المثال، إذا لم تشعر بالراحة لتقول شيئا في غرفة مليئة بالأشخاص، فينبغي أن لا يُقال ذلك الشيء عبر البريد الإلكتروني).

٥,٤ قواعد و سلوكيات الإنترنت

لن يتم التسامح باستخدام أنظمة جامعة الإمام محمد بن سعود الإسلامية للقيام بأي استخدام مسيء، أو غير أخلاقي أو "غير ملائم" للإنترنت و قد يشكل ذلك أساسا للإجراءات التأديبية، بما في ذلك إنهاء العمل. و تشمل الأمثلة على الإستخدام غير الملائم للإنترنت من قبل الموظفين، على سبيل المثال لا الحصر، التالي:

- القيام بالأنشطة غير القانونية أو المشاركة فيها.
- الدخول على مواد إباحية أو تحميلها.
- إستدعاء العروض التعاقدية التي ليست معتمدة من الإدارة.

- الكشف عن الملكية أو معلومات سرية أو نشرها.
- التصريح بآراء شخصية تمس جامعة الإمام محمد بن سعود الإسلامية.
- الإدلاء بتصريحات غير لائقة أو نشرها.
- تحميل أو تنزيل برمجيات تجارية بما يخالف ترخيصها.
- تحميل الوثائق السرية الخاصة بجامعة الإمام محمد بن سعود الإسلامية أو إرسالها عبر البريد الإكتروني دون تصريح من الأطراف المعنية.
- تنزيل أي برمجيات أوملفات إلكترونية دون وجود تدابير معقولة للحماية من الفيروسات.
- إستخدام ملقم إنترنت (Proxy) غير المستخدم و المعتمد من عمادة تقنية المعلومات.

٥,٥ المحظورات على أنشطة المستخدم على الإنترنت

لمنع أي مظهر من مظاهر السلوك غير اللآئق على الإنترنت و للحد من الخطر على الجامعة، على المستخدمين تجنب التالي:

- استخدام شعارات جامعة الإمام محمد بن سعود الإسلامية أو موادها الداخلية في أي صفحة إلكترونية أو نشرها على الإنترنت مالم تتم الموافقة على ذلك مقدما من قبل الإدارة.
- استخدام ملفات البرمجيات، و الصور، أو أي معلومات أخرى يتم تنزيلها من الإنترنت والتي لم يتم إصدارها للإستخدام العام المجاني.
- عرض المواد المخلة بالأخلاق، أو المسيئة، أو تلك المتعلقة بإنتاج، و استخدام، أو تخزين أو نشر المواد الجنسية أو الخليعة على شبكة أو أنظمة جامعة الإمام محمد بن سعود الإسلامية.

- محاولة الحصول على صلاحيات غير قانوني على الأنظمة البعيدة على الإنترنت.
- محاولة الدخول على حاسوب شخص آخر ضمن نفس الشبكة بشكل غير صحيح أو إجراء المسح على منافذ الأنظمة البعيدة على الإنترنت.
- استخدام أو حيازة أدوات المسح الأمني أو تقييم ضعف الأمن, دون الحصول على إذن من مسؤول أمن المعلومات.
- نشر المواد بما يخالف قانون حقوق الطبع و النشر.
- إنشاء إتصالات للإنترنت أو أي شبكة خارجية أخرى من شأنها أن تسمح للمستخدمين غير المصرح لهم بالدخول إلى أنظمة جامعة الإمام محمد بن سعود الإسلامية و أصول معلوماتها , ومن ذلك استخدام برمجيات الدخول لجهاز الحاسب من خلال الإنترنت (مثل برنامج Team Viewer).

٥,٦ الإتصالات غير المصرح بها

لا يسمح لمستخدمي أي جهاز حاسب يرتبط بشبكة جامعة الإمام محمد بن سعود الإسلامية الربط على شبكة الإنترنت من خلال وسائل إتصال غير مصرح بها.

٥,٧ المعلومات الحساسة

- لا يتم نقل المعلومات السرية عبر الإنترنت دون وجود التدابير الأمنية (مثل التشفير). ويتم استخدام خوارزمية التشفير المعتمدة من قبل مسؤول أمن المعلومات لحماية هذه المعلومات.

- لا يتم إرسال أرقام البطاقات الإئتمانية، و أرقام بطاقات الإتصال الهاتفي، و أسماء المستخدمين و كلمات السر الخاصة بتسجيل الدخول، والمعطيات الأخرى التي يمكن استخدامها للدخول على الأنظمة، عبر الإنترنت على شكل نص عادي "غير مشفر".

٥,٨ استضافة الموظف لمواقع إلكترونية خاصة

لا يُسمح للموظفين بإنشاء صفحات إلكترونية أو مواقع إلكترونية تشير إلى جامعة الإمام محمد بن سعود الإسلامية أو االفروع والمعاهد التابعة لها، أو تتخفى تحت اسم جامعة الإمام محمد بن سعود الإسلامية أو تكشف بأي طريقة عن أي معلومات تتعلق بجامعة الإمام محمد بن سعود الإسلامية دون الإذن الخطي من الإدارة. ولا يُسمح للموظفين باستضافة مواقع شخصية على منشآت جامعة الإمام محمد بن سعود الإسلامية.

٥,٩ كلمات المرور

- ينبغي أن تستوفي كافة كلمات المرور وهويات المستخدمين على الإنترنت معايير كلمة المرور لدى جامعة الإمام محمد بن سعود الإسلامية على النحو الموضح في سياسة أمن كلمة المرور.
- تجنب كتابة كلمة المرور الخاصة بك أو الاحتفاظ بها بطريقة غير آمنة وفي الحالات التي تضطر فيها لتدوين كلمة المرور الخاصة بك يجب الاحتفاظ بكلمة المرور في موقع آمن، كما يجب طمسها بشكل سليم عندما تنتفي الحاجة لذلك.
- يجب ألا يتم تبادل كلمة المرور مع أي شخص بما في ذلك موظفي قسم أنظمة التشغيل في عمادة تقنية المعلومات.
- تجنب استخدام نفس كلمة المرور في حسابات مختلفة.
- مع أن استخدام نفس كلمة المرور مع حسابات مختلفة يجعل من السهل تذكرها، فإنه قد يكون لها كذلك تأثير متسلسل يسمح للمهاجمين بالوصول إلى أنظمة تشغيل متعددة.

- تجنب استخدام خاصية الوصول التلقائي. استخدام خاصية الوصول التلقائي تلغي من أهمية استخدام كلمة المرور.

٥,١٠ مسح الفيروسات

يتم فحص كافة البيانات والبرمجيات التي يتم تنزيلها على أنظمة الحاسب في جامعة الإمام محمد بن سعود الإسلامية عبر الإنترنت بأنظمة مضاد الفيروسات والبرامج الخبيثة قبل استخدامها. يرجى الرجوع إلى سياسة الحماية من الفيروسات.

٦. استخدام البريد الإلكتروني

٦,١ الاستخدام للعمل فقط

يتم استخدام أنظمة البريد الإلكتروني لأغراض العمل فقط، مالم توافق إدارة الجامعة بشكل خاص على الاستخدام في مجال غير ذلك.

٦,٢ التعامل مع البريد الإلكتروني بسرية

على موظفي جامعة الإمام محمد بن سعود الإسلامية التعامل مع رسائل البريد الإلكتروني والملفات على أنها معلومات سرية. ويتم التعامل مع البريد الإلكتروني كمراسلات سرية و مباشرة بين المرسل و المستقبل.

٦,٣ حقوق الإدارة في الإطلاع على محتوى البريد الإلكتروني

عند حدوث مخالفة أمنية أو استدعت الحاجة لتحقيق أمني، تمتلك عمادة تقنية المعلومات في جامعة الإمام محمد بن سعود الإسلامية، و مسؤول أمن المعلومات ، أو فريق التدقيق الحق في فحص البريد الإلكتروني، وأدلة الملف الشخصي، و المعلومات الأخرى المخزنة على أجهزة الحاسوب الخاصة بجامعة الإمام محمد بن سعود الإسلامية وذلك بعد أخذ الإذن من صاحب الصلاحية. حيث

يضمن هذا الفحص الإمتثال للسياسة الأمنية و الداخلية لجامعة الإمام محمد بن سعود الإسلامية، و يدعم أجراء التحقيقات الداخلية، ويساعد في إدارة أنظمة معلومات جامعة الإمام محمد بن سعود الإسلامية.

٦,٤ القيود على نقل المعلومات الحساسة

على المستخدمين عدم إرسال المعلومات السرية أو الحساسة عبر البريد الإلكتروني مالم يتم تشفير المادة باستخدام تقنيات التشفير المعتمدة من قبل إدارة أمن المعلومات.

٦,٥ التشارك بخدمات البريد الإلكتروني

ينبغي على موظفي جامعة الإمام محمد بن سعود الإسلامية استعمال البريد الإلكتروني الخاص بهم و عدم استخدام أو الدخول إلى حساب البريد الإلكتروني الذي تم تعيينه لفرد آخر سواء لإرسال أو إستقبال الرسائل. وإذا كانت هناك حاجة لقراءة البريد الإلكتروني الخاص بشخص آخر (أثناء وجوده في إجازة على سبيل المثال)، يتم بدلا عن ذلك استخدام تمرير الرسالة و غيرها من التسهيلات.

٦,٦ تمرير البريد الإلكتروني

مالم يتم الحصول على موافقة مالك المعلومات مقدما، أو مالم تكن المعلومات متاحة للعامة بشكل واضح بطبيعتها، لا يقوم الموظفين بتمرير البريد الإلكتروني لأي عنوان خارج شبكة جامعة الإمام محمد بن سعود الإسلامية.

٦,٧ بيانات سجلات البريد الإلكتروني

يتم الاحتفاظ بسجل رسائل البريد الإلكتروني المرجعية لمدة أطول عند حدوث إجراءات تحقيق في مخالفات أمنية .

٦,٨ التخلص من بيانات البريد الإلكتروني

في الوقت الذي تشجع فيه عمادة تقنية المعلومات على وجود نسخ إحتياطية من المعلومات الموجودة على الحاسب، إلا أنه ينبغي التخلص من المراسلات الداخلية عندما تنتهي الحاجة إليها. ويتم تخزين رسائل البريد الإلكتروني ذات العلاقة بالأنشطة الحالية أو تلك المتوقع أن تصبح ذات علاقة بالأنشطة الحالية، كملفات منفصلة ويتم الإحتفاظ بها وفقا لسياسة الاحتياط والاسترداد.

يجب على مستخدمي جامعة الإمام محمد بن سعود الإسلامية عدم استخدام خدمات البريد الإلكتروني لأي من الأغراض التالية:

- استخدام البريد إلكتروني للمراسلات الشخصية, وكذلك استخدام البريد الشخصي لمراسلات العمل.
- إرسال رسائل بريد إلكتروني غير مرغوب فيها أو متطفلة، وخاصة ذات الطبيعة التجارية.

٧. الوصول عن بعد (VPN)

- يجب استخدام الوصول عن بعد لأغراض العمل فقط.
- يُسمح لأعضاء مجتمع الجامعة باستخدام صلاحية الوصول عن بعد للخدمات الموكلة لهم فقط.
- يخضع الوصول عن البعد لنظام التأكد من كلمة المرور باستخدام نظام الجامعة العادي.
- إمكانية الوصول للمعلومات تكون باستخدام عملية تسجيل آمنة.
- دخول الأجهزة عن بعد يكون عرضة للتسجيل والمراقبة.
- تجنب الدخول عن بعد إلى شبكة الجامعة الخاصة باستخدام أجهزة أو شبكات عامة غير موثوقة أو أثناء التواجد في أماكن عامة.
- وجود نسخة أصلية من برنامج حماية من الفايروسات (Anti-virus) محدَّث ومدعوم من الشركة المصنعة.
- استخدام البرنامج المصرح من ادراة أمن المعلومات وعدم استخدام برمجيات الدخول لجهاز الحاسب من خلال الإنترنت (مثل برنامج Team Viewer)
- التواصل مباشرة مع إدارة أمن المعلومات في حالة ملاحظة شك بوجود تهديد أمن سيبراني.

٨. الالتزام

على كافة موظفي جامعة الإمام محمد بن سعود الإسلامية ، و المقاولين، و المستشارين، والموظفين المؤقتين و غيرهم من العاملين ومنسوبي الجامعة التقيد بسياسة أمن المعلومات (القبول بالاستخدام الآمن لتقنية المعلومات).

الوثائق ذات العلاقة

تعتبر هذه السياسة مرتبطة بسياسات جامعة الأمام محمد بن سعود الأسلامية ممثله في عمادة تقنية المعلومات الخاصة بالوصول والتحكم بالشبكة والوصول عن بعد وهي أيضا مرتبطة بسياسات والضوابط الأساسية للهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية ، وبسياسة استخدام الشبكة الخاصة الافتراضية والتشريعات والسياسات الصادرة عن الهيئة الوطني للأمن السيبراني، كما هو موضح في الجدول التالي:

م	الاسم	الوصول	رابط الوصول
١	الضوابط الأساسية للأمن السيبراني	Online	https://nca.gov.sa/files/ecc-ar.pdf
٢	ضوابط الأمن السيبراني للعمل عن بعد	Online	https://www.nca.gov.sa/files/wfh-ar.pdf

٩. مراجع السياسة

٩,١ مراجع سياسات جامعة الإمام محمد بن سعود الإسلامية

- إدارة الأصول
- أمن أجهزة الحاسب المحمولة و أجهزة الحاسب المكتبية
- أمن الشبكات
- أمن البريد الإلكتروني
- صلاحيات الوصول إلى شبكة الإنترنت

٩,٢ مراجع ISO27001

- الاستخدام المقبول للأصول (A.7.1.3)
- سياسات و إجراءات تبادل المعلومات (A.10.8.1)
- إرسال الرسائل الإلكترونية (A.10.8.4)
- حظر إساءة استخدام أنظمة معالجة المعلومات (A.15.1.5)