جامعة فهد بن سلطان
FAHAD BIN SULTAN UNIVERSITY

سياسة الخصوصية والاستخدام

أولا/ سياسات استخدام موارد تقنيه المعلومات

الهدف:

تهدف هذه اللوائح الى تنظيم وتحديد مسؤوليات المستخدم والاستخدام المعتمد لتعزيز الاستخدام الفعال والقانوني والأخلاقي لأنظمة تقنية المعلومات والاتصالات في الجامعة والحفاظ علي سرية البيانات والملفات والأصول والشبكات وكذلك حماية حقوق الملكية الفكرية والبرمجيات المستخدمة في الجامعة.

التعريفات:

يكون للكلمات التالية حيثما وردت في هذه اللوائح المعاني المخصصة لها أدناه ما لم تدل القرينة على غير ذلك:

المستخدم: أي شخص يستخدم البوابة الإلكترونية المملوكة للجامعة.
الشبكة: الشبكة المحلية المستخدمة داخل الجامعة بشقيها السلكي واللاسلكي.
البريد الإلكتروني الرسمي: البريد الممنوح لمنسوبي الجامعة والطلبة من قبل وحدة تكنولوجيا المعلومات في الجامعة.

أنظمة تقنية المعلومات والاتصالات:

أنظمة تقنية المعلومات والاتصالات وكل المعلومات الواردة في هذه ا لأنظمة هي ملك للجامعة ويكون المستخدم مسؤولًا عنها، وفي حال تم تسريبها، أو العبث بها، فإن هذا سوف يؤدي إلى نتائج سلبية تشمل) ولكن لا تقتصر على) الخسارة المالية أو تعطيل الأعمال.

الملكية تشمل: بيانات العملاء و الموردين، قوائم الموظفين، المعلومات المالية مثل التكاليف والاستثمارات والأرباح والمبيعات والتوقعات، استراتيجيات المبيعات والتسويق، الأجور، المرتبات، الاستحقاقات، طلبات الحصول على المعلومات المقترحة، ملفات الموظفين، بما في ذلك السجلات، التعويض، خطط العمل والأهداف والمبيعات والخدمات، وخطط التدريب.

أنظمة تقنية المعلومات والاتصالات المتوفرة في الجامعة هي لأغراض العمل فقط، ويسمح للموظفين باستخدامها فقط عند الضرورة لتحقيق أهداف الوظيفة أو لمتطلبات المهام الموكلة إليهم مع التأكد من استخدامها بمستوى عالٍ من الحرص والرعاية . الاستخدام الشخصي لهذه ا لأدوات والاتصالات مسموح في حدود المعقول وعلى التقدير المناسب من إدارة تقنية المعلومات في الجامعة.

جامعة فهد بن سلطان
FAHAD BIN SULTAN UNIVERSITY

سياسة الخصوصية والاستخدام

تحتفظ الجامعة بالحق في مراقبة جميع جوانب الاتصالات ونظم المعلومات في أي وقت دون سابق إنذار، وعلاوة على ذلك اتخاذ إ جراءات تأديبية، بدءًا من إلغاء الوصول للشبكة أو الخدمة إلى التوصية بالإقالة وذلك في حال عدم الالتزام بما ورد في هذه الوثيقة . إن القواعد والشروط المذكورة في هذه الاتفاقية تطبق على جميع الأفراد الذين يستخدمون أنظمة الاتصالات والمعلومات في الجامعة.

الإجراءات والسياسات:

معالجة البيانات المصنفة (الخاصة أو السرية):

أ) يجب على المستخدم عدم معالجة المعلومات المصنفة (الخاصة او السرية) التي تخص الجامعة على أي جهاز ما لم تتم الموافقة عليه و تحديد المستوى الامني المناسب.

ب) يجب على المستخدم إبلاغ مدير تقنية المعلومات عن أي استخدام لأي برنامج أو نظام غير الأنظمة المعتمدة في الجامعة.

ج) يجب على المستخدم عدم حفظ وتخزين المعلومات التي تخص الجامعة على أجهزته الشخصية أو أي أدوات أخرى دون الموافقة على ذلك.

كلمات المرور:

أ) يجب على المستخدم حماية كلمات ورموز الأمان وعدم إفصاحها للغير أو فقدانها في جميع الأوقات.

ب) يجب على المستخدم استخدام كلمة مرور يصعب تخمينها وذلك بما لا يقل عن ثمانية أحرف كحد أدنى تتكون من(أرقام، علامات خاصة، أحرف كبيرة وصغيرة).

ج) يجب تغيير كلمة المرور الافتراضية أو المحددة مسبقاً الخاصة بالمستخدم على الفور عند تسجيل الدخول لأول مرة بعد تزويده بها.

د) يجب حفظ كلمات المرور في مكان امن أو عدم مشاركتها مع الآخرين.

ه) لا ينبغي أن تتكرر كلمة المرور المستخدمة سابقًا أو مبنية من بيانات شخصية واضحة مثل (الاسم الأخير، أرقام الهواتف، أسماء الأقارب أو اسم حيوان أليف، وما إلى ذلك).

حسابات المستخدم:

أ) يحظر تماما مشاركة حساب المستخدم مع الآخرين أو الوصول لحسابات الآخرين.

ب) يحظر على المستخدم محاولة الوصول إلى الحسابات أو البيانات غير المصرح له بها.

ج) المستخدم مسؤول عن جميع الإجراءات المتخذة بموجب اسم الحساب الخاص به.

د) يجب على المستخدم عدم استخدام أي حساب على جهاز اللاب توب أو جهاز مكتبي غير الممنوح له من قبل وحدة تقنية المعلومات.

جامعة فهد بن سلطان
FAHAD BIN SULTAN UNIVERSITY

سياسة الخصوصية والاستخدام

حماية البيانات:

أ) يجب على المستخدم التعامل مع وسائط التخزين وفقًا لأعلى مستوى من حماية البيانات والأمان، مثال عدم تعريضها للحقول الكهرومغناطيسية القوية.

ب) يجب على المستخدم في حال الوصول إلى أي معلومات مصنفة(سرية أو خاصة)،ابلاغ وحدة تقنية المعلومات لكي يتم تخزينها بطريقة آمنة ومحمية تمنع غير المصرح لهم بالوصول لها.

ج) يجب على المستخدم حماية البيانات التي تخص الجامعة ولا يتم مشاركتها مع أي أفراد غير المرخص لهم.

الأمن المادي:

أ) يجب على المستخدم عدم إزالة أنظمة معلومات الجامعة أو برمجياتها بدون إذن خطي من مدير تقنية المعلومات.

ب) يكون المستخدم مسؤولًا عن المراقبة والمحافظة على أي أجهزة محمولة، أجهزة رقمية شخصية أو أقراص مدمجة تخص الجامعة في عهدته، و يخضع للمسائلة عنها في حالة التلف أو الضياع.

ج) يتحمل المستخدم كامل المسؤولية في حالة سرقة أو فقدان البيانات، وعليه في هذه الحالة إبلاغ وحدة تقنية المعلومات على الفور، كما يتوجب عليه دائماً الاحتفاظ بنسخة احتياطية للبيانات المهمة.

د) يجب على المستخدم تسجيل جميع الأجهزة الشخصية التي يملكها ويريد استعمالها للوصول الى موارد تقنية المعلومات وذلك بعد موافقة وحدة تقنية المعلومات.

ه) يجب على الموظف تسليم كافة الأجهزة أو الأنظمة التي تخص الجامعة (والتي كانت تحت عهدته أثناء عمله في الجامعة) عند الإستقالة أو نهاية العقد.

البريد الإلكتروني:

أ) تقوم الجامعة بتزويد كل موظف في الجامعة بالبريد الإلكتروني الرسمي الخاص به.

ب) تكون جميع عناوين البريد الإلكتروني التابعة لجامعة فهد بن سلطان، والمستخدمة من قبل الجامعة بهدف التواصل بين الجامعة والجهات الأخرى، أو التواصل داخل الجامعة ملكًا خاصًا للجامعة.

ج) يعد البريد الإلكتروني الرسمي للجامعة، وسيلة تواصل رسمية معتمدة لجميع منسوبي الجامعة.

د) توفر الجامعة نظام البريد الإلكتروني فقط لاستخدامات العمل الرسمي، وفقًا لذلك، يجب على المستخدم عدم استخدامه لأمور شخصية أو الاشتراك به على أي مواقع أخرى.

ه) يجب على الموظف أن يقوم بفتح بريده الإلكتروني مرة واحدة على الأقل كل 24 ساعة، و يستثنى من ذلك وقت الإجازات الرسمية والإجازات السنوية للموظف، مالم يطلب منه المسؤول المباشر أن يكون على اتصال معه أثناء الإجازة على أن يتم إصدار قرار مكتوب بذلك من الجهة المسؤولة.

و) يجب على المستخدم تضمين توقيعه في جميع المراسلات الرسمية وتحديث توقيعه باستمرار من خلال مطابقته مع سجلات نظام إدارة الموارد البشرية.

ز) يتحمل الموظف كامل المسؤولية عن البريد الإلكتروني الرسمي الخاص به.

ح) لا يسمح للموظفين، وتحت أي ظرف من الظروف بتبادل أسماء المستخدمين وكلمات المرور فيما بينهم.

ط) يجب على المستخدم عدم إرسال رسالة بريد إلكتروني تحتوي على مصطلحات (خبيثة، عدائية، تهديد، إفساد،ابتذال، افتراء، تدنيس أو عنصرية، جنسية أو عرقية) كما يجب عليه أن يتقدم بتقرير على الفور في حال تلقيه أي بريد إلكتروني يحتوي عليها.

ي) يجب على المستخدم عدم فتح أي مرفقات لرسائل البريد الإلكتروني مالم يتم معرفة مصدرها والوثوق بها تجنبًا للخطر المرفق من إحتوائه على فيروسات أو برامج ضاره أخرى.

ك) يتم حذف البريد الإلكتروني الرسمي للموظف بعد انتهاء خدمته من الجامعة.

استخدام الأنترنت:

أ) يقتصر الوصول إلى الشبكات العامة و (الإنترنت) على العمل الرسمي فقط.

ب) يجب على المستخدم تقييد الوصول غير الرسمي للإنترنت لمنع التداخل مع واجباته الرسمية أو التسبب في التأثير على أداء خدمة الشبكة.

ج) يجب على المستخدم عدم الوصول إلى المواقع التي تحتوي على محتويات (خبيثة، عدائية، تهديد،إفساد، ابتذال، افتراء، تدنيس أو عنصرية، جنسية أو عرقية)أو رسومات ونصوص غير مقبوله أخلاقيًا.(برامج وأدوات التواصل الاجتماعي والتقنيات على شبكة الإنترنت والهاتف النقال، هي منصات ووسائل فعاله للتواصل مع الآخرين سواء على المستوى الشخصي أو المهني ومع ذلك فمن الضروري استخدام وسائل الاتصال الاجتماعي بعناية مع الامتثال للقواعد المذكورة أعلاه لتجنب سوء الاستخدام).

د) يجب على المستخدم إبلاغ موظفي تقنية المعلومات فورًا عند فشل حجب المواقع غير المرغوب فيها، يجب على المستخدم الالتزام بجميع قواعد وسياسات أمن استخدام الإنترنت التي تم وضعها من إدارة تقنية المعلومات وعدم استخدام أي تطبيق من مثل(Hotspot ,VPN , Torrent) لأنها تؤدي إلى الاختراق الأمني.

الشبكة والاتصال عن بعد:

أ) يلتزم المستخدم الذي يرغب في الاتصال بالشبكة باستخدام الأجهزة المملوكة له شخصيًا، بالبرمجيات المصرح له بها فقط والتي يتم تفعيلها وبموافقة مسبقة من قبل وحدة تقنية المعلومات.

ب) يجب على المستخدم عدم الاتصال بأي اجهزة داخل الشبكة في مكان العمل أو الأنظمة وذلك باستخدام برنامج TeamViewer أو الاتصال عن بعد(عن طريق أي أداة أخرى)لأي سبب من الأسباب دون موافقة مسبقة من وحدة تقنية المعلومات.

حماية البيانات المعروضة:

أ) يجب على المستخدم إغلاق أجهزته عند ترك مكان العمل غير المراقب لفترات طويلة (أو الفترة بين نهاية الدوام ودوام اليوم التالي)، مالم يأذن مسؤول وحدة تقنية المعلومات.

ب) يجب على المستخدم تفعيل قفل الحساب أو شاشة محمية بكلمة مرور والتي تتطلب إعادة إدخال كلمة المرور عندما يكون النظام خاملًا لفترة قصيرة من الزمن.

نظام مكافحة الفيروسات (حماية نقطة النهاية):

أ) يتحمل المستخدم مسؤولية اتخاذ الإجراءات المناسبة لضمان تحديث برنامج مكافحة الفيروسات التي قامت الجامعة بتوفيرها لكافة اجهزة الحاسب، وعلى المستخدم التأكد أن النظام محمي من الفيروسات. ويشمل ذلك فحص الملفات والبيانات على وسائط التخزين الخارجية.

ب) يجب على المستخدم إبلاغ مدير وحدة تقنية المعلومات عن أي احتمال أو مخاوف من مصدر أو محتوى الأقراص المدمجة أو الفلاش ميموري أو مرفقات البريد الإلكتروني.

ج) يجب على المستخدم إبلاغ مدير تقنية المعلومات فورًا في حال وجود أي مؤشر على وجود فايروس أو تهديد أمني آخر.

حماية حقوق النشر:

أ) يجب على المستخدم عدم تحميل أو تثبيت برامج أو إزالة برامج لها حقوق نشر أو رخص خاصة بالجامعة دون إذن خطي من مدير النظام أو مدير تقنية المعلومات.

ب) يتحمل المستخدم كامل المسؤولية عن أي انتهاكات لحقوق نشر أو تراخيص للبرمجيات التي تم تنصيبها على أجهزة الجامعة و التي يتم استخدامها من قبله.

ج) تعد تراخيص البرامج و الأجهزة ملك للجامعة، وعلية يجب عدم استخدامها على أجهزه خاصة أو مشاركتها مع الآخرين.

د) يقتصر استخدام الاتصالات وأنظمة تقنية المعلومات للجامعة على الأشخاص المرخص لهم فقط، أي شخص يدخل هذا النظام دون إذن أو تجاوز الدخول المصرح به أو ينتهك شروط استخدام المرافق وموارد تقنية المعلومات يمكن أن يخضع لإجراءات تأديبية أو قانونية، أو الاثنين معاً في إطار القانون.

ثانيا /سياسة حماية البيانات الشخصية

الهدف:

يحتاج مركز التعلم الإلكتروني إلى جمع واستخدام البيانات الشخصية للمستخدمين من الطلاب والموظفين والأفراد الآخرين الذين يتعاملون مع المركز. حرصت جامعه فهد بن سلطان علي حمايه حقوق الخصوصية للمستخدمين عند معالجتها لذلك تم عمل هذي السياسة والتي تمنح قوانين حماية البيانات حقوقاً للأفراد بالإضافة إلى مسؤوليات أولئك الذين يعالجون البيانات الشخصية.

التعريفات:

البيانات: مجموعة من المعلومات في صورتها الحقيقية أو في صورة غير منظمة مثل الفيديو أو التسجيلات الصوتية أو الرموز التعبيرية.

البيانات الشخصية:

كل بيان -مهما كان مصدره أو شكله- من شأنه أن يؤدي إلى الوصول لمعرفه الشخص على وجه التحديد، أو يجعله قابلاً للوصول اليه بصفة مباشرة أو غير مباشرة عند اضافه هذي البيانات مع بيانات أخرى.

التحقق:

عمليه يتم من خلالها التأكد من هويه الفرد او جهاز او جهاز باعتباره مطلب أساسي للسماح باستخدام الموارد التقنية.

معالجه البيانات الشخصية:

هي عمليه يتم من خلالها جمع بيانات المستخدم باي وسيله كانت علي سبيل المثال لا الحصر (جمع البيانات ونقلها وتخزينها ومشاركتها وتحليلها والسعي الي ربطها مع بيانات اخري واتلافها.

صاحب البيانات الشخصية:

الفرد الذي تتعلق به البيانات الشخصية أو من يمثله أو المفوض عنه

جامعة فهد بن سلطان
FAHAD BIN SULTAN UNIVERSITY

سياسة الخصوصية والاستخدام

السياسات:

أ) لا تقوم الجامعة بجمع البيانات الشخصية إلا إذا قدمها المستخدم مثل التسجيل في ورش العمل أو المشاركة في النقاشات أو التقديم على وظائف معلن عنها، وتعتبر موافقة ضمنية وسرية ومحمية للمدة اللازمة وللجامعة صلاحيه الاطلاع على هذه البيانات، ولن تتم مشاركتها إلا بموافقة المستخدم، ويمكن تصفح الموقع دون تسجيل الدخول ولا يمكن التعرف على معلومات الشخصية مثل الاسم أو رقم الهاتف أو البريد الإلكتروني.

ب) تحرص الجامعة علي حماية البيانات الشخصية من التسرب، أو التلف، أو الفقدان، أو الاختلاس، أو إساءة الاستخدام، أو التعديل أو الوصول غير المصرح به

ج) تحرص الجامعة علي الاحتفاظ بالبيانات الشخصية بصورة دقيقة، وكاملة، وذات علاقة مباشرة بالأغراض التي جمعت من اجلها

د) للجامعة صلاحيه الاحتفاظ بالبيانات حسب المدة التي تراها بناء علي الأغراض التي جمعت من اجلها

ه) لأصحاب المصلحة في الجامعة صلاحيه الاطلاع على البيانات التي سيتم جمعها من الافراد حيث لن تتم مشاركة أي بيانات إلا بموافقة الشخص.

و) لصاحب البيانات الحق في الوصول إلى بياناته الشخصية والتأكد من أن معالجه بياناته بصوره عادلة وقانونية.وله الحق في طلب تعديل بياناته اذا كانت غير مكتملة وكذلك يحق له الاعتراض علي معالجه بياناته اذا كان الغرض من المعالجة أداء مهمه المصلحة العامة.

ز) قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في الجامعة.

ح) لإدارة الجامعة إصدار التعليمات التنفيذية اللازمة لتطبيق هذا النظام.

ط) تبت إدارة الجامعة في الحالات التي لم يرد فيها نص واضح والإشكاليات التي قد تنتج عن تطبيق مواد هذه اللائحة.

ي) وكيل الجامعة ومساعد الوكيل لشؤون مركز الحاسب ومدير المركز مسؤولون عن تنفيذ هذه اللائحة.

ك) تلغى هذه اللائحة أي لوائح أو تعليمات أو قرارات سابقة بهذا الشأن اعتبارا من تاريخ اعتمادها.