إطار سياسات استخدام تقنية المعلومات بكلية الإعلام بجامعة صنعاء

تمهيد:

تعتبر السياسة بيان رسمي لمبدأ أو قاعدة يجب أن تتبع من طرف الأعضاء المنتمين لأي منظمة كانت كلية أو جامعة او إدارة تقنية المعلومات المختصة، إذ تحدد كل سياسة أهمية كل مهمة أو عملية سيتم تنفيذها داخل المنظمة أو في علاقتها مع محيطها، في حين أن الإجراء يخبر أعضاء المنظمة بكيفية تنفيذ السياسة المتفق عليها، والتي يجب أن يتم ضبطها في شكل خطوات مرتبة وواضحة ومحددة، وعلى هذا الأساس اتجهت وحدة الجودة بكلية الإعلام، جامعة صنعاء، لوضع سياسات وإجراءات خاصة بها تضمن تنفيذ المهام المناطة بعهدتها بكفاءة وفاعلية لتحقيق الأهداف الاستراتيجية للوحدة والكلية والجامعة ككل، وتحدد هذه المدونة الإطار العام للمبادئ الأخلاقية وقواعد استخدام التقنية التي يتعين على أعضاء هيئة التدريس وموظفي الكلية الاسترشاد بها، وهذه القواعد هي كما يلي:

١. تُعتبر الحواسيب والشبكات ونظم المعلومات الإلكترونية موارد أساسية لتحقق الجامعة والكلية رسالتها في التدريس والبحث العلمي وخدمة الجامعة والمجتمع. وتمنح الجامعة والكلية أعضائها حق الدخول إلى تقنيات المعلومات بغية دعم تحقيق رسالتها.

٢. تُعد هذه الموارد مرافق قيمة للجامعة والكلية وينبغي استخدامها وإدارتها على نحو مسؤول لضمان أمنها وسلامتها وإتاحتها للأنشطة التعليمية المناسبة، وعلى كافة مستخدمي هذه الموارد أن يستخدموها بشكل مسؤول وفاعل.

٣. يتحمل المستخدمون بالجامعة والكلية مسؤولية معرفة حقوقهم وواجباتهم تجاه هذه السياسة التي توضح المسؤولية في الاتصالات الشخصية والمسائل الأمنية وتحدد عواقب المخالفات، ويُعتبر المستخدمون مسؤولين عن تعريف أنفسهم بأية متطلبات إضافية تتعلق بكليتهم أو الوحدة التي ينتمون إليها.

٤. يجب على المستخدمين معرفة حقوق ومسؤوليات استخدام مرافق الحوسبة السحابية العامة. هذه المدونة تحدد المسؤوليات المتعلقة بالاتصالات الشخصية والقضايا الأمنية وقضايا الخصوصية عند استخدام الخدمات السحابية العامة.

٥. يتحمل مستخدمو مرافق تقنية المعلومات بالكلية والجامعة مسؤولية محتوى اتصالاتهم الشخصية، ويمكن أن يقعوا تحت طائلة المسؤولية من جراء هذا الاستخدام، ولا تتحمل الجامعة أو الكلية أي مسؤولية عن الاستخدام الشخصي أو غير المسموح به لمواردها عن طريق أي من المستخدمين.

٦. لا تستخدم البيانات أو المعلومات والنظم إلا من قبل الأشخاص المخول لهم استخدامها للقيام بمهام تتعلق بأداء أعمالهم، ويمنع استخدام المعلومات والنظم لمكاسب أو أعمال شخصية أو لارتكاب أعمال الغش.

٧. يحظر على المستخدمين الإفصاح أو الكشف عن أية معلومات دون تفويض أو تخويل رسمي، ويشكل الولوج غير المسموح به للمعلومات أو التلاعب بها أو الإفصاح عنها أو تسريبها خرقاً أمنياً قد يؤدي إلى اتخاذ عمل تأديبي يصل إلى إنهاء الخدمة والملاحقة القضائية من قبل الجهات الحكومية.

٨. على المستخدمين الإلمام بحقوق ومسؤوليات مستخدمي الكلية والجامعة. وتحدد هذه المدونة الخطوط العريضة لمسؤولية الاتصالات الشخصية، وقضايا الأمن والخصوصية، كما تحدد عواقب الانتهاكات.

٩. يجب استخدام خدمات الإنترنت لأغراض العمل فقط.

١٠. يحظر الدخول للمواقع المحظورة أو ذات المحتوى المحظور وفقاً لسياسة الجامعة.

١١. على المستخدم عدم الدخول للمواقع المسيئة أو المساهمة فيها أو تحميل ملفات منها، وتشمل هذه المواقع المسيئة ولا تقتصر على: مواقع تروج للعنصرية، مواقع دينية ذات مشاعر تعصبية، مسيئة، أو ذات لغة عدائية، تشهيرية، أو مسيئة لفرد أو جماعة، أو ذات محتوى إباحي.

١٢. على مستخدمي الإنترنت عدم المساهمة في أي نشاط قد يسهم في إيقاف عمليات أنظمة الحاسب الآلي.

١٣. على مستخدمي الإنترنت عدم تحميل أو تنزيل أو تثبيت برمجيات من الإنترنت بدون الموافقة المسبقة من إدارة نظم المعلومات.

١٤. على المستخدمين عدم تركيب أي شبكات افتراضية خاصة أو استخدام برمجيات بالوكالة بهدف الالتفاف على سياسة أمن الشبكات بالجامعة.

١٥. على الموظف أو عضو هيئة التدريس الذي تم تزويده بجهاز حاسوب مراعاة ما يلي:

- **اتخاذ كافة الإجراءات اللازمة للحفاظ على الحاسوب الخاص به.**
- **عدم تنزيل البرامج على الجهاز إلا بعد مراجعة إدارة نظم المعلومات والصيانة.**
- **التأكد من إطفاء الجهاز قبل مغادرة مكان العمل.**

- **المحافظة على سرية المعلومات الموجودة على الجهاز الخاص به من خلال استعمال كلمة السر الخاصة به وعدم إفشائها للغير.**
- **عدم استخدام الجهاز لأغراض التسلية وعدم تنزيل الألعاب والبرامج الترفيهية.**
- **عدم الدخول إلى أجهزة الآخرين ومحاولة الحصول على معلومات منها.**
- **استخدام الجهاز لغايات تطوير المهارات والقدرات وبما يتلاءم مع مصلحة العمل.**
- **عدم استخدام الجهاز لإنجاز أعماله الشخصية.**
- **ترشيد استخدام الطابعات قدر الإمكان.**

١٦. على الموظف أو عضو هيئة التدريس الذي تتوفر لديه إمكانية الوصول إلى شبكة الانترنت مراعاة ما يلي:

- **الالتزام باستخدامها لأغراض العمل بما في ذلك لغايات تطوير القدرات والمهارات ذات العلاقة بطبيعة عمله وبما يصب في مصلحة العمل.**
- **الالتزام بشروط ومتطلبات حقوق الملكية الفكرية للملفات والبرامج ومراعاة شروط ترخيص استخدامها.**
- **استشارة الوحدة المعنية بنظم المعلومات والصيانة فوراً لدى ملاحظة أية أمور غير طبيعية خلال استخدام الانترنت.**
- **عدم تنزيل النصوص والصور التي تحتوي على مواد غير أخلاقية، أو عنصرية، أو تحتوي على آراء سياسية متطرفة، أو تحرض على العنف والكراهية، أو أية أنشطة غير قانونية.**
- **عدم تنزيل الملفات التي لا تتعلق بطبيعة عمله مباشرة كملفات الفيديو وملفات الوسائط المتعددة، مثل الأفلام أو الأغاني، أو الموسيقى وما شابه ذلك.**
- **عدم استخدام الجهاز والانترنت لمحاولة الدخول والتسلل إلى أجهزة وشبكات أخرى. وعدم استخدام الانترنت لإرسال مواد سرية، أو سياسية، أو تحتوي على تهديد ومضايقة للآخرين.**

٣. على الموظف أو عضو هيئة التدريس أو الطالب الذي يخصص له عنوان بريد الكتروني مراعاة ما يلي:

- **عدم استخدام البريد الالكتروني لإنشاء وتوزيع الرسائل التي تحتوي على مواد دعائية، أو شخصية، أو لا أخلاقية، أو تلك التي تتضمن آراء سياسية متطرفة أو تعليقات عنصرية حول المعتقدات والممارسات الدينية أو النوع الاجتماعي، أو العمر، أو العرق، وفي حال ورود أية رسالة من أي موظف أو عضو هيئة تدريس أو طالب بهذا الخصوص يجب إبلاغ الوحدة المعنية بنظم المعلومات عن ذلك مباشرة.**
- **عدم إعادة إرسال الرسائل التي تصله وتحتوي على النكات أو الصور أو ملفات الأفلام والصور ذات الحجم الكبير.**
- **عدم إعادة إرسال الرسائل الواردة والتي قد تحتوي على فيروسات أو ملفات قد يشتبه بأنها فيروسات، ويجب في هذه الحالة الاستعانة بالوحدة المعنية بأنظمة المعلومات.**
- **الأخذ بعين الاعتبار بأنه ليس هنالك أية خصوصية فيما يتعلق بالرسائل التي تصل إلى أي موظف أو عضو هيئة تدريس أو التي يرسلونها من خلال نظام البريد الالكتروني. ويجوز الرقابة على البريد الالكتروني لأي موظف أو عضو هيئة تدريس من قبل موظفين مصرح لهم دون إخطار مسبق.**
- **عدم فتح أية رسائل واردة غير معروفة أو غير متوقعة، حتى لو كانت الرسالة من شخص معروف لدى الموظف وكذلك عدم فتح أو تنزيل أية ملفات مرفقة يشك في مصدرها.**
- **استخدام البريد الالكتروني لتطوير القدرات والمهارات وفقاً لمتطلبات العمل.**

حقوق وواجبات ومسؤوليات المستخدم

١. يصرح لأعضاء أسرة الكلية والجامعة باستخدام موارد تقنية المعلومات بغية تسهيل أنشطتهم العلمية والبحثية والوظيفية المتعلقة بالجامعة؛ بيد أن المستخدمين يوافقون باستخدامهم هذه الموارد على التقيد والالتزام بكل إجراءات وسياسات الجامعة في المجالات التي تتضمن على سبيل المثال لا الحصر المضايقات، والسرقة الأدبية، والاستخدام التجاري، والأمن الإلكتروني، والتصرف غير الأخلاقي، والقوانين التي تحظر السرقة والخروقات المتعلقة بحقوق الطبع والتراخيص، والتدخلات غير القانونية، وقوانين سرية البيانات.

٢. تنطبق هذه القيود والالتزامات بسياسات الجامعة في هذا المجال على الضيوف المصرح لهم باستخدام موارد تقنية المعلومات الخاصة بالجامعة.

٢. تقع على عاتق المستخدمين مسؤولية ما يلي:

١. استعراض وفهم كل السياسات والإجراءات والقوانين المتعلقة بالدخول واستخدام موارد تقنية المعلومات والتقيد بها.

٢. الاستفسار من مدراء النظم أو الأمناء على البيانات عن توضيح سبل الدخول أو الاستخدام المقبول والآمن لموارد تقنية المعلومات في الجامعة.

٣. الإبلاغ عن أي خروقات للسياسة المعتمدة للجهات المعنية أو للسلطة الإدارية المختصة.

٣. المسؤولية عن الاتصالات الشخصية:

يعتبر مستخدمو موارد تقنية المعلومات في الجامعة مسؤولين عن محتوى اتصالاتهم الشخصية. ولا تقبل الجامعة أي مسؤولية عن أي استخدام شخصي أو غير مصرح به لمواردها من قبل مستخدميها.

٤. السرية والوعي الأمني:

يجب أن يعي المستخدمون أن الجامعة لا تضمن السرية أو الأمن الإلكتروني المطلقين رغم اتخاذها إجراءات أمنية جيدة لحماية أمن مواردها الحاسوبية وحساباتها الخاصة بأعضائها، ويجب على المستخدمين أن يتبعوا الإجراءات الأمنية المناسبة.

٥. الحوسبة السحابية:

يجب أن يتوافق استخدام خدمات الحوسبة السحابية العامة مع جميع السياسات والإجراءات المنصوص عليها في الجامعة. وتقع مسؤولية استخدام هذه الخدمات على عاتق العاملين لضمان أن عملية الاستخدام تتوافق مع السياسات المتبعة في الجامعة، وعلاوة على الالتزام بالقواعد والسياسات ذات الصلة يجب مراعاة الإجراءات الآتية عند استخدام خدمات الحوسبة السحابية:

١. الخصوصية وأمن البيانات:

لا يجوز استخدام الحوسبة السحابية لتداول أي معلومات تم تصنيفها وفق سياسة تصنيف المعلومات في الجامعة على أنها معلومات سرية أو شخصية أو خاصة أو حساسة.

١. متطلبات أخرى:

يجب على أعضاء هيئة التدريس والموظفين والطلبة بجامعة صنعاء توخي الحذر الشديد عند القيام بالاستخدام الذاتي للخدمات السحابية في معالجة أو تخزين أو تبادل أو إدارة أي بيانات مؤسسية.

تنطوي جميع الخدمات السحابية على مخاطر تتعلق بإدارة البيانات الهامة التي قد تتعرض للمخاطر أو التغيير بدون إشعار، ولذلك فمن المفترض أن جميع الخدمات السحابية تتطلب من المستخدمين الفرديين الإذعان لاتفاقيات محددة والموافقة على شروط معينة من خلال النقر على الروابط. ولا تسمح هذه الاتفاقيات للمستخدمين بالتفاوض على أي شروط واردة ولا توفر أي فرصة لشرح أو توضيح الشروط، وغالباً يتم تقديم هذه الشروط والضمانات في سياقات غامضة. وفي معظم الأحيان يتم تغيير الشروط دون سابق إنذار. وتشتمل عملية الاستخدام الذاتي للخدمات السحابية على المخاطر التالية:

- **ضعف المراقبة على الدخول والافتقار إلى قواعد الأمن العامة.**
- **الفقدان الفجائي للخدمة بدون سابق إنذار.**
- **الفقدان الفجائي للبيانات دون سابق إنذار.**
- **إمكانية العبث بالبيانات المخزنة والتي تم معالجتها من خلال الخدمات السحابية، ويمكن إعادة بيع هذه البيانات من خلال طرف ثالث مما يشكل تهديداً للخصوصيات.**
- **قد تنجم مخاطر تحيق بحقوق الملكية الفكرية الحصرية والمتعلقة بالبيانات المخزنة والتي تم معالجتها من خلال الخدمات السحابية.**

١. تبعات الخروقات والمخالفات:

لا يتم إيقاف امتيازات استخدام موارد تقنية المعلومات في الجامعة دون سبب، ويجوز للجامعة أن توقف الدخول مؤقتاً لبعض الموارد إذا تبين لها أثناء التحري أنه ضروري لحماية سلامة وأمن حواسيبها وشبكاتها. ويتم إحالة المخالفات المزعومة للسياسة للجهة المعنية في الجامعة، وبناءً على طبيعة وخطورة المخالفة قد يتسبب ذلك في سحب امتيازات الدخول أو إجراء تأديبي من قبل الجامعة أو الملاحقة الجنائية.

فقدان البيانات:

المستخدمون مسؤولون عن عمل نسخ احتياطية من ملفاتهم الخاصة، كما يجب ألا يفترضوا وجود نسخ احتياطية لتلك الملفات على أجهزتهم. ويتعين على المستخدمين الحفاظ على نسخ احتياطية وأرشفتها وذلك بالنسبة للبيانات الهامة على أجهزتهم، علماً بأن رسائل البريد الإلكتروني المحذوفة والتي تكون أقدم من ٣٠ يوماً غير قابلة للاسترداد؛ كما أن استرداد رسائل البريد الإلكتروني المحذوفة هو خدمة ذاتية، يتم تنفيذها بواسطة مالك البريد الإلكتروني.

الاستخدام والمسؤوليات:

١. المستخدم هو المسؤول عن حماية والمحافظة على المعلومات المخزنة في الحاسب المكتبي والحاسب المحمول من الضرر، أو السرقة أو الضياع.

٢. في حالة سرقة الحاسب المحمول/الهاتف النقال، يجب على المستخدم إبلاغ الشرطة ونظم المعلومات في الجامعة على الفور.

٣. حالة ضرر أو ضياع الحاسب المحمول/ الهاتف النقال، يجب على المستخدم إبلاغ نظم المعلومات.

٤. يجب على المستخدم عدم ترك الحاسب المحمول/ الهاتف النقال في الأماكن العامة دون مراقبة.

٥. يجب استخدام كلمة مرور حماية لإغلاق الشاشة للحاسب المحمول/ الهاتف النقال بعد الانتهاء من استخدامهما.

٦. يجب على المستخدم عدم توصيل أجهزة الحاسب الآلي الشخصية على شبكة الجامعة.

٧. يجب على المستخدم عدم تغير الوظائف الإدارية في الحاسب المحمول بأي شكل من الأشكال، مثل نظام التشغيل في الجهاز، أو تعريف مسؤول النظام، وكلمة المرور.

٨. يجب على المستخدمين إكمال نسخ / دعم بياناتهم المرتبطة بهوية الدخول التي يتم توفيرها من قبل الجامعة قبل آخر يوم عمل / التخرج من الجامعة.