الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة وهران 1 أحمد بن بلة

ميثاق تكنولوجيا المعلومات

معتمد من مكتب استراتيجية الرقمنة

توطئة:

تقدم جامعة وهران 1 أحمد بن بلة لمستخدميها (طلبة، أساتذة، وموظفين) إمكانيات وموارد تكنولوجيا المعلومات لتمكينهم من القيام بالمهام المنوطة والموكلة إليهم بأحسن وجه. بهدف تطوير وتعزيز التكوين الأولي والمتواصل وتثمين البحث العلمي وتشجيع العمل الجامعي التعاوني. يزيد الاستخدام غير السليم والسيء لهذه الوسائل من مخاطر حدوث انتهاكات تهدد أمن وسلامة أنظمة معلومات الجامعة.

في إطار تنفيذ المرجع الوطني لأمن المعلومات، و لضمان سرية وسلامة وتوافر، تقرر وضع ميثاق أمن تكنولوجيا المعلومات على أساس المرجع الوطني لأمن المعلومات وسائر النصوص المعمول بها في هذا المجال، من أجل زيادة المستوى الأمني للنظام المعلوماتي للجامعة.

المادة الأولى: الهدف

تهدف جامعة وهران 1 من خلال هذا الميثاق إلى تحديد شروط ومبادئ وكيفية استخدام الموارد المعلوماتية (الأجهزة والبرمجيات). كما يحدد قواعد الأمن المعلوماتي التي يجب على المستخدمين احترامها.

المادة 02: الهيئة المعنية

يسري ويطبق هذا الميثاق على كل شخص يستخدم بشكل دائم أو مؤقت الموارد المعلوماتية لجامعة وهران 1.

المادة 03: ملكية الموارد المعلوماتية

- ✓ جميع الموارد المعلوماتية المتاحة والموضوعة تحت المستخدمين هي ملكية حصرية لجامعة وهران 1 دون غيرها.
- ✓ جميع البيانات والمعلومات المخزنة في معدات وأجهزة جامعة وهران 1 أو التي تنتقل والمتبادلة عبر شبكاتها هي ملكية حصرية للجامعة.

المادة 04: شروط استخدام والولوج إلى الموارد والشبكات المعلوماتية

يخضع كل استخدام للموارد وشبكات المعلوماتية بالجامعة لإجراءات التحقق من الهوية (اسم المستخدم وكلمة المرور) مسبقة.

المادة 05: مسؤولية المستخدم

المستخدم هو المسؤول الوحيد عن أي استخدام للوسائل التي توفرها له الجامعة.

المادة 06: حماية وسائل المعلوماتية

للحفاظ على الوسائل الموضوعة تحت تصرف المستخدم، يجب على هذا الأخير :

- ✓ السعي لضمان حماية وحفظ المعلومات السرية المستخدمة الخاصة؛
- ✓ تغيير كلمات المرور الخاصة بشكل دوري؛
- ✓ لا تترك كلمة المرور مطلقا في مجال يمكن للآخرين الوصول أليه؛
- ✓ تأكد من تأكيد تسجيل الخروج قبل مغادرة الحاسوب أو مختلف المنصات؛
- ✓ قم بتغيير كلمة المرور عند أي شك في حدوث قرصنة للنظام المعلوماتي الخاص بك؛
- ✓ لا تعط كلمة مرورك أبدا، حتى للأشخاص المسؤولين عن الأمن المعلوماتي للنظام؛
- ✓ لا تقم أبدا بإرسال كلمة المرور الخاصة بك عن طريق الهاتف أو البريد الإلكتروني.

المادة 07: استخدام الموارد المعلوماتية

- ✓ لا يسمح باستخدام الموارد المعلوماتية الخاصة بجامعة وهران 1 إلا للأغراض المهنية.
- ✓ يجب على المستخدم الحفاظ على الموارد المعلوماتية (المعلومات والوسائل) الموضوعة تحت تصرفه.
- ✓ لا يحق للمستخدم تسجيل أو نشر التطبيقات أو البرمجيات على أجهزة الحاسوب المتاحة له من قبل الجامعة.
- ✓ في حالة تعطل أو حدوث خلل في هذه الأجهزة، يجب على المستخدم إبلاغ المصلحة المسؤولة عن الصيانة فوراً.

المادة 08: إلتزامات جامعة وهران 1 نحو المستخدمين

يجب على جامعة وهران 1 ما يلي :

- ✓ توفير للمستخدم الموارد المعلوماتية الضرورية لأداء المهام الموكلة إليه على أحسن وجه.
- ✓ توفير للمستخدم الموارد المعلوماتية وضمان السير الحسن لها.
- ✓ الحفاظ على الجودة الخدمات المقدمة للمستخدمين في حدود الإمكانات المتاحة.
- ✓ إبلاغ المستخدمين بالإجراءات والسياسات والطرق المعمول بها في مجال الموارد المعلوماتية.
- ✓ توفير الوسائل اللازمة لضمان سرية وسلامة معلومات وبيانات المستخدمين والتبادلات الإلكترونية.
- ✓ إعلام المستخدمين بأن الأنشطة على الشبكة والأنظمة تخضع للمراقبة الآلية.
- ✓ توعية المستخدمين بالمخاطر المتعلقة بأمن أنظمة المعلومات.

المادة 09: إلتزامات المستخدم

يجب على المستخدم أن يحترم ما يلي:

- ✓ احترام القوانين والتشريعات المعمول بها فيما يتعلق بالموارد المعلوماتية وأمن المعلومات.
- ✓ احترام هذا الميثاق وكذلك الإجراءات والالتزامات المختلفة لجامعة وهران 1.
- ✓ تطبيق إجراءات وتوجيهات أمن تكنولوجيا المعلومات الخاصة بالجامعة بدقة.
- ✓ عدم استخدام أو استغلال حسابات للآخرين.
- ✓ الإبلاغ فورا عن أي عمليات مشبوهة أو حوادث أمنية على الفور.

المادة 10: أمن وحماية مكان العمل

يجب على المستخدم أن يحترم بدقة تعليمات الأمن والسلامة التالية:

- ✓ إغلاق الحاسوب أو محطة العمل في حالة الغياب، أو حتى الغياب المؤقت.
- ✓ تنبيه وإبلاغ مصلحة الإعلام الآلي في حالة اكتشاف أجهزة جديدة متصلة بجهاز العمل.
- ✓ التأكد من أن جهاز الحاسوب مزود ببرنامج مكافحة الفيروسات، وإبلاغ المصلحة المعنية بأي تنبيه أمني.
- ✓ لا تقم بتوصيل المعدات الشخصية المستخدمة في الاتصالات بحاسوب العمل.
- ✓ فحص جميع وسائط التخزين الخارجية ضد الفيروسات قبل استخدامها.
- ✓ إيقاف تشغيل الحاسوب أثناء فترات التوقف عن العمل أو الراحة الطويلة (الليل، عطلة نهاية الأسبوع، الأعياد، الإجازة...).
- ✓ عدم فتح أو محاولة صيانة الأجهزة (فتح الوحدات المركزية، وما إلى ذلك)، وإذا لزم الأمر اتصل بمصلحة الصيانة.

المادة 11: استخدام البريد الإلكتروني المهني

توفر الجامعة للمستخدمين حسابات البريد الإلكتروني المهني، تتيح لهم إرسال واستقبال الرسائل الإلكترونية ذات الطابع المهني.

لا يسمح باستخدام البريد الإلكتروني المهني إلا لأغراض العمل. ولهذه الغاية، يمنع منعا باتا القيام بما يلي:

- ✓ استخدامه لأغراض غير مهنية (شخصية أو حزبية).
- ✓ استخدامه للتسجيل في شبكات التواصل الاجتماعي والمنتديات والمواقع الإلكترونية التي ليس لها علاقة بالأهداف المهنية للمستخدم.
- ✓ فتح المرفقات والروابط الفائقة المرسلة من حساب بريد إلكتروني غير معروف.

- ✓ فتح البريد الإلكتروني المهني من فضاءات عامة ومفتوحة للإنترنت، ولا سيما مقاهي الإنترنت.
- ✓ لا تقم بإدخال معلومات تسجيل الدخول للفضاءات المهنية الخاصة بك على استمارة لموقع واب مجهول. يجب التأكد جيدا من عنوان الموقع قبل تسجيل الدخول.

عندما تتطلب المهام الاستثنائية للمستخدم تسجيله على شبكات التواصل الاجتماعي والمنتديات والمواقع الإلكترونية، يتم إنشاء عنوان بريد إلكتروني مخصص لهذا الغرض بعد الحصول على موافقة السلطة المسؤولة المخولة لذلك.

يجب على المستخدم توخي الحذر عند إرسال رسائل عن طريق البريد الإلكتروني وذلك من خلال التأكد من:

- ✓ صياغة وكتابة عنوان المرسل إليه بشكل صحيح.
- ✓ المرسل إليه يجب ان يكون مؤهل للاطلاع على محتوى المعلومات المرسلة.
- ✓ التأكد من إرفاق الملفات الصحيحة بالرسالة لتفادي إرفاق ملفات عن طريق الخطأ

يمنع منعا باتاً استخدام عناوين البريد الإلكتروني الشخصية لإرسال المستندات المهنية.

المادة 12: استخدام الإنترنت

يوافق المستخدمون الذين لديهم اتصال أو بإمكانهم الولوج إلى الإنتنرنت على عدم :

- ✓ تعمد استخدام واستغلال هذه الخدمات لأغراض خبيثة، بديئة أو تصفح مواقع عنصرية أو تشهيرية أو إباحية أو غير قانونية.
- ✓ تقديم معلومات تتعلق بوظائفهم أو رتبهم أو مسؤولياتهم على وسائل التواصل الاجتماعي.
- ✓ الإفراط في تحميل الملفات باستخدام شبكة الجامعة (تنزيل ملفات ذات أحجام كبيرة).
- ✓ توخي الحذر عند تنزيل الملفات، والتأكد من فحصها باستخدام أحد برمجيات مكافحة الفيروسات.

المادة 13: الأجهزة المحمولة ووسائط التخزين القابلة للإزالة (USB)

يجب على المستخدم :

- ✓ إبلاغ المسؤول المباشر في التسلسل الهرمي فوراً عن أي فقدان أو سرقة لجهاز محمول أو أحد وسائط تخزين المعلومات المهنية (USB).
- ✓ القيام بغلق وإيقاف تشغيل الأجهزة المحمولة عندما لا تكون قيد الاستخدام.
- ✓ القيام بإلغاء وظائف Wi-Fi وBluetooth الخاصة بالأجهزة عندما لا تكون ضرورية.

- ✓ يمنع نقل المستندات عن طريق أجهزة (USB) من طرف أي شخص غير منتسب للجامعة، في هذه الحالات يجب أن يتم تبادل المستندات عن طريق البريد الإلكتروني. وفي حالة كون حجم البيانات كبير يتطلب استخدام أجهزة (USB)، لكن يجب فحص الأجهزة من قبل المصلحة المختصة قبل أي استخدام.
- ✓ تشفير البيانات السرية الموجودة في الأجهزة المحمولة وأجهزة التخزين (USB).
- ✓ أثناء تنقلات العمل، يجب على المستخدم الاحتفاظ بأجهزته المحمولة وأجهزة التخزين (USB) معه.

المادة 14: تدابير الأمن الواجب تطبيقها عند التنقل نحو الخارج

- ✓ يحظر استخدام الأجهزة غير المخصصة للمهمة المهنية (أجهزة الحاسوب والأجهزة اللوحية) للدخول إلى حساب البريد الإلكتروني المهني أو المنصات الرقمية.
- ✓ يجب على المكلف بالمهمة المهنية أن يحرص على إبقاء الأجهزة المهنية بصحبته في جميع الأوقات والتنقلات،
- ✓ القيام بإلغاء وظائف Wi-Fi وBluetooth الخاصة بالأجهزة عندما لا تكون ضرورية.
- ✓ يجب حذف جميع البيانات المهنية الحساسة، غير الضرورية للمهمة، من جميع الأجهزة المحمولة وأجهزة التخزين (USB) قبل أي رحلة إلى الخارج.
- ✓ يجب إبلاغ المسؤولين بالجامعة، والتمثيل الدبلوماسي الجزائري بالخارج في حالة تفتيش أو حجز أجهزة الحاسوب من قبل السلطات الأجنبية أثناء البعثات في الخارج.ذ
- ✓ يحظر استخدام المعدات والأجهزة المقدمة كهدية أثناء الرحلة إلى الخارج للأغراض المهنية.
- ✓ يذكر في تقارير المهمة قائمة المعدات والأجهزة المقدمة كهدية خلال الرحلة.
- ✓ يمنع منعاً باتاً نقل المستندات من قبل شخص أجنبي عبر وسائط تخزين (USB). يجب أن يتم أي تبادل للوثائق حصريا عن طريق البريد الإلكتروني.
- ✓ تغيير كلمات المرور السرية المستخدمة أثناء المهمة بالخارج.

المادة 15: نهاية علاقة المستخدم بجامعة وهران 1

- ✓ عندما تنتهي العلاقة بين المستخدم وجامعة وهران 1، يجب على المستخدم أن يعيد إلى الجامعة جميع موارد وأجهزة تكنولوجيا المعلومات الممنوحة له.
- ✓ عندما تنتهي العلاقة بين المستخدم وجامعة وهران 1، تقوم هذه الأخيرة بحذف أية صلاحيات وحقوق لاستخدام والولوج إلى الموارد المعلوماتية التي توفرها له المصلحة.

المادة 16: إدارة الحوادث

في حالة حدوث مشكل يمكن أن يؤثر على أمن نظام المعلومات يمكن للجامعة :

- ✓ عزل المستخدم، بإشعار أو من دونه حسب خطورة الوضع أو الموقف.
- ✓ العزل أو التحييد المؤقت لأي بيانات أو ملفات تتعارض مع ميثاق تكنولوجيا المعلومات أو من شأنه أن يعرض أمن أنظمة معلومات الجامعة للخطر.
- ✓ إبلاغ المسؤول المباشر.

المادة 17: عدم الإلتزام بالميثاق

من المرجح أن يؤدي عدم الامتثال أو عدم احترام للقواعد المحددة في هذا الميثاق إلى تحميل المستخدم مسؤوليته ويؤدي إلى اتخاذ إجراءات تأديبية ضده بما يتناسب مع خطورة الأفعال التي تم تسجيلها.

شريطة أن يتم إبلاغ المسؤول المباشر، يمكن لمسؤولي أمن تكنولوجيا المعلومات :

- ✓ إبلاغ وتحذير المستخدم.
- ✓ إلغاء صلاحيات المستخدم أو تجميدها مؤقتا.
- ✓ حذف أو ضغط أو عزل كل البيانات أو الملفات التي تتعارض مع الميثاق أو من شأنها أن تعرض أمن أنظمة المعلومات للخطر.

مع عدم الإخلال بالعقوبات التأديبية، يمكن إخضاع أي شخص ينتهك أحكام هذا الميثاق لإجراءات المتابعة القضائية.

المادة 18: سريان مفعول ميثاق تكنولوجيا المعلومات

يدخل ميثاق تكنولوجيا المعلومات حيز التنفيذ فور نشره على الموقع الويب الرسمي لجامعة وهران 1، أو بمجرد عرضه على المستخدم بمجرد قيامه بالولوج إلى الشبكة المحلية للجامعة، أو بمجرد توقيع المستخدم عليه.،كما يتم إبلاغ كافة المستخدمين بمحتوى الميثاق عبر البريد الإلكتروني المهني. أي رفض للتوقيع سيحظر استفادة المستخدم من وسائل تكنولوجيا المعلومات الخاصة بجامعة وهران 1.