الجمهوريـــــــة الجزائريـــــــة الديمقراطيـــــــة الشعبيـــــــة
République Algérienne Démocratique et Populaire

وزارة التعليم العالي و البحث العلمي

جـــامعة 20 أوت 1955 سكيكـــــدة

مركز الأنظمة و شبكات الإعلام و الاتصال
و التعـــليم المتلفـــز و التعلـــيم عن بعد

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

---

Université 20 août 1955 - SKIKDA

Centre des Systèmes et Réseaux d'Information et de Communication, de Télé-enseignement et d'Enseignement à Distance

الميثاق الداخلي لتكنولوجيا الإعلام والاتصال

يرجى قراءة الميثاق بعناية مع التوقيع على التعهد في الصفحة الأخيرة

مقدمة

توفر جامعة سكيكدة لمستخدميها إمكانيات ووسائل الإعلام الآلي لتمكينهم من إنجاز المهام الموكلة إليهم. يزيد الاستخدام غير السليم لهذه الوسائل من مخاطر حدوث انتهاكات لأمن أنظمة معلومات الجامعة.

في إطار تنفيذ المرجع الوطني لأمن المعلومات ، تقرر إثراء ميثاق أمن تكنولوجيا الإعلام والاتصال القديم، الذي اعتمدته جامعة سكيكدة ، من أجل زيادة المستوى الأمني للنظام المعلوماتي للمؤسسة.

المادة 1 : الهدف

الغرض من هذا الميثاق هو تحديد شروط و مبادئ استخدام موارد الإعلام الآلي (الأجهزة والبرامج) في جامعة سكيكدة. كما يحدد قواعد الأمن المعلوماتي التي يجب على المستعملين اتباعها.

المادة 2 : الهيئة المعنية

يسري هذا الميثاق على أي شخص يستخدم بشكل دائم أو مؤقت موارد الإعلام الآلي في جامعة سكيكدة.

المادة 3 : ملكية موارد تكنولوجيا المعلومات

- جميع موارد الإعلام الآلي المتاحة للمستخدمين هي ملكية حصرية لجامعة سكيكدة ؛
- جميع البيانات و المعلومات المخزنة على أجهزة جامعة سكيكدة أو المتبادلة عبر شبكاتها هي ملكية حصرية للجامعة.

المادة 4 : شروط استخدام الموارد و شبكات الإعلام الآلي

يخضع كل استخدام لموارد وشبكات الإعلام الآلي بالجامعة لإجراءات التحقق من الهوية (اسم المستخدم وكلمة المرور) مسبقا.

المادة 5 : مسؤولية المستعمل

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

المادة 6 : حماية وسائل الإعلام الآلي

حفاظاً على الوسائل المتاحة للمستعمل ، يجب على هذا الأخير :

- السعي لضمان حماية وحفظ المعلومات السرية الخاصة من خلال مراعاة النقاط التالية :
  - لا تترك كلمة المرور مطلقًا في مجال يمكن للآخرين الوصول إليه ؛
  - لا تستخدم أبدًا نفس كلمة المرور على منصات مختلفة؛
  - 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.
  - تغيير كلمات المرور الخاصة بك بشكل دوري.
- يُمنع منعًا باتًا مشاركة و كشف كلمات المرور الخاصة بك مع جهات خارجية :
  - لا تعطِ كلمة مرورك أبدًا ، حتى للأشخاص المسؤولين عن الأمن المعلوماتي للنظام ؛
  - لا تقم أبدًا بإرسال كلمة المرور الخاصة بك عن طريق الهاتف أو البريد الإلكتروني أو الرسائل الفورية.

المادة 7 : استخدام وسائل الإعلام الآلي

- لا يسمح استخدام وسائل الإعلام الآلي الخاصة بالمؤسسة إلا للأغراض المهنية ؛
- يجب على المستعمل الحفاظ على موارد و وسائل الإعلام الآلي (المعلومات والوسائل) المتاحة له ؛
- لا يحق للمستعمل تسجيل أو نشر تطبيقات أو برمجيات على أجهزة الحاسوب الممنوحة له بالجامعة. يمكن فقط لمصلحة الإعلام الآلي تنفيذ هذه المهمة؛
- في حالة تعطل هذه الأجهزة ، يجب إبلاغ المصلحة المسؤولة عن الصيانة على الفور.

المادة 8 : التزامات المؤسسة تجاه المستعملين

يجب على المؤسسة :

- توفير وسائل الإعلام الآلي الضرورية للمستعمل لأداء المهام الموكلة إليه ؛
- توفير موارد تكنولوجيا الإعلام وضمان السير الحسن لها؛
- الحفاظ على جودة الخدمة المقدمة للمستعملين في حدود الإمكانيات المتاحة.
- إبلاغ المستعملين بالإجراءات و الطرق المعمول بها في مجال موارد تكنولوجيا الإعلام والاتصال ؛
- توفير الوسائل اللازمة لضمان سرية وسلامة معلومات وبيانات المستعملين والتبادلات الإلكترونية؛
- إعلام المستعملين بأن الأنشطة على الشبكة والأنظمة تخضع للمراقبة الآلية؛
- توعية المستعملين بالمخاطر المتعلقة بأمن أنظمة المعلومات.

المادة 9 : التزامات المستعمل

يجب على المستعمل :

- احترام القوانين المعمول بها فيما يتعلق بوسائل الإعلام الآلي والأمن المعلوماتي ؛
- احترام هذا الميثاق وكذلك الإجراءات والالتزامات المختلفة للمؤسسة ؛
- تطبيق إجراءات وتوجيهات أمن تكنولوجيا الإعلام الخاصة بالجامعة بدقة ؛
- عدم استخدام أو استغلال حسابات الولوج للآخرين؛
- الإبلاغ عن أي عمليات مشبوهة أو حوادث أمنية على الفور.

المادة 10 : سلامة وحماية مكان العمل

يجب على المستعمل أن يحترم بدقة تعليمات السلامة التالية :

- إغلاق الحاسوب في حالة الغياب ، أو حتى الغياب المؤقت.
- تنبيه مصلحة الإعلام الآلي في حالة اكتشاف أجهزة جديدة متصلة بجهاز العمل (الحاسوب)؛
- منع الاتصال بالشبكات عن بعد غير المصرح بها : تعطيل خاصية "سطح المكتب عن بعد"، لا تستخدم برمجيات الاتصال عن بعد مثل TeamViewer ، تعطيل اكتشاف الشبكة عبر الانترنت ، استخدام ميزة "Privé" بالنسبة لخصائص الشبكة؛
- التأكد من أن جهاز الحاسوب مزود ببرنامج مكافحة الفيروسات، وإبلاغ المصلحة المعنية بأي تنبيه أمني؛
- لا تقم أبدًا بتوصيل المعدات الشخصية المستخدمة في الاتصالات بحاسوب العمل؛
- فحص جميع المعدات المتصلة بحاسوب العمل ضد الفيروسات قبل استخدامها ؛
- إيقاف تشغيل الحاسوب أثناء فترات التوقف عن العمل لفترة طويلة (ليلاً، عطلة نهاية الأسبوع، و الإجازة)؛
- عدم فتح أو صيانة الجهاز (فتح الوحدات المركزية ، وما إلى ذلك). إذا لزم الأمر اتصل بمصلحة الصيانة.

المادة 11 : استخدام البريد الإلكتروني المهني

توفر الجامعة للمستعملين حسابات البريد الإلكتروني المهني التي تتيح لهم إرسال واستقبال الرسائل الإلكترونية ذات الطابع المهني.

لا يسمح باستخدام البريد الإلكتروني المهني إلا لأغراض العمل. ولهذه الغاية، يُمنع منعًا باتًا :

- استخدامه لأغراض غير مهنية؛
- استخدامه للتسجيل في شبكات التواصل الاجتماعي و المنتديات والمواقع الإلكترونية التي لا علاقة لها بالهدف المهني للمستعمل؛
- فتح المرفقات أو روابط الانترنت المرسلة من حساب بريد إلكتروني غير معروف؛
- فتح البريد الالكتروني المهني من فضاءات عامة و مفتوحة للإنترنت، ولا سيما مقاهي الإنترنت أو عبر شبكات Wi-Fi العامة ؛

- لا تقم أبدًا بإدخال معلومات تسجيل الدخول للفضاءات المهنية الخاصة بك على إستمارة لموقع واب مجهول (Hameçonnage). يجب التأكد جيدا من عنوان الموقع قبل تسجيل الدخول.

عندما تتطلب المهام الاستثنائية للمستخدم تسجيله على الشبكات الاجتماعية أو المنتديات أو المواقع الإلكترونية ، يتم إنشاء عنوان بريد إلكتروني مخصص لهذا الغرض بعد الحصول على موافقة السلطة المسؤولة المخولة لذلك.

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

- صياغة عنوان المرسل إليه بشكل جيد ؛
- المرسل إليه يجب أن يكون مؤهل للاطلاع على محتوى المعلومات المرسلة ؛
- التأكد من إرفاق الملفات الصحيحة بالرسالة لتفادي إرفاق مستندات عن طريق الخطأ.

يُمنع منعًا باتًا استخدام عناوين البريد الإلكتروني الشخصية لإرسال المستندات المهنية؛

المادة 12 : استخدام الإنترنت

بصرف النظر عن ضرورة تشفير البيانات، يتم مراقبة الاتصال بالإنترنت على مستوى الجامعة عن طريق حسابات لكل المستخدمين، ويتحمل كل مستعمل مسؤولية كل نشاط مرتبط بحسابه الخاص للاتصال بالإنترنت.

يوافق المستعملون الذين لديهم اتصال بالإنترنت على عدم :

- تعمد استخدام هذه الخدمة لأغراض خبيثة أو احتيالية أو تصفح مواقع عنصرية أو تشهيرية أو إباحية أو غير قانونية ؛
- تقديم معلومات تتعلق بوظائفهم أو رتبتهم أو مسؤوليتهم على الشبكات الاجتماعية ؛
- الإفراط في تحميل الملفات باستخدام شبكة الجامعة (تنزيل ملفات ذات أحجام كبيرة)؛
- توخي الحذر عند تنزيل الملفات، والتأكد من فحصها باستخدام أحد برامج مكافحة الفيروسات.

ومع ذلك، فإن الاستخدام الشخصي المحدود يبقى مقبول. يجب أن يتوافق هذا الاستخدام مع معايير ممارسات الأمن المعلوماتي.

المادة 13 : الأجهزة المحمولة وأجهزة التخزين USB

يجب على المستعمل :

- إبلاغ المسؤول المباشر في التسلسل الهرمي فورًا عن أي فقدان لجهاز محمول مهني أو سرقته أو جهاز تخزين المعلومات المهني USB ؛
- القيام دائمًا بغلق الأجهزة المحمولة عندما لا تكون قيد الاستخدام؛
- القيام بإلغاء وظائف Wi-Fi و Bluetooth للأجهزة عندما لا تكون ضرورية؛
- حظر نقل المستندات عن طريق جهاز USB من طرف أي شخص غير منتسب للجامعة، في هذه الحالة يجب أن يتم تبادل أي مستند عن طريق البريد الإلكتروني. في حالة كون حجم البيانات يتطلب استخدام جهاز USB، يجب فحص الجهاز من قبل المصلحة المختصة قبل أي استخدام؛
- تشفير البيانات السرية الموجودة في الأجهزة المحمولة و أجهزة التخزين USB؛
- أثناء تنقلات العمل، يجب على المستعمل الاحتفاظ بأجهزته المحمولة معه.

المادة 14 : إجراءات الأمن المعلوماتي الواجب اتخاذها عند السفر إلى 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 و Bluetooth للأجهزة 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 التفتيش أو الاستيلاء على أجهزة الحاسوب من قبل السلطات الأجنبية أثناء البعثات في الخارج؛
- يحظر استخدام المعدات و الأجهزة المقدمة أثناء رحلة إلى الخارج للأغراض المهنية (إلا للمهام المكلف بها)؛
- يذكر في تقارير المهمة قائمة المعدات و الأجهزة المقدمة خلال الرحلة ؛
- يُمنع منعًا باتًا نقل المستندات من قبل شخص أجنبي عبر وسائط تخزين USB. يجب أن يتم أي تبادل للوثائق حصريًا عن طريق البريد الإلكتروني ؛
- تغيير كلمات المرور المستخدمة أثناء المهمة.

المادة 15 : انتهاء العلاقة بين المستعمل و الإدارة

- عندما تنتهي العلاقة بين المستعمل والإدارة، يجب على المستعمل أن يعيد إلى المؤسسة جميع موارد وأجهزة تكنولوجيا المعلومات الممنوحة له؛
- تقوم المؤسسة بحذف أية صلاحيات لاستخدام موارد الإعلام الآلي التي توفرها له المصلحة.

المادة 16 : إدارة الحوادث

في حالة وقوع حادث يمكن أن يؤثر على الأمن المعلوماتي، يمكن للإدارة :

- عزل المستخدم، بإشعار أو بدونه حسب خطورة الموقف؛
- العزل أو التحييد المؤقت لأي بيانات أو ملف يتعارض مع الميثاق أو من شأنه أن يعرض أمن أنظمة المعلومات للخطر؛
- إبلاغ السؤول المباشر.

المادة 17 : عدم الالتزام بالميثاق

من المرجح أن يؤدي عدم الامتثال للقواعد المحددة في هذا الميثاق إلى تحميل المستعمل 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 و تحذير المستعمل؛
- إلغاء صلاحيات المستعمل أو تجميدها مؤقتًا ؛
- حذف أو عزل أي بيانات أو ملف يتعارض مع الميثاق أو من شأنه أن يعرض أمن أنظمة المعلومات للخطر.

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

المادة 18 : الدخول حيز التنفيذ

يدخل هذا الميثاق حيز التنفيذ بمجرد توقيع المستخدم عليه. أي رفض للتوقيع سيحظر استفادة المستخدم من وسائل تكنولوجيا المعلومات الخاصة بالمؤسسة.

تعهد

يرجى قراءة الميثاق بعناية

سيدي سيدتي،

نذكرك أنه بصفتك منتسبا (أستاذا، موظفا أو طالب دكتوراه) إلى الجامعة، يتعين عليك احترام القواعد المعمول بها في المؤسسة من حيث موارد تكنولوجيا الإعلام والأمن المعلوماتي.

كما ندعوك للامتثال للممارسات الجيدة لاستخدام البريد الإلكتروني والإنترنت، المنصوص عليها في ميثاق تكنولوجيا الإعلام والاتصال.

بموجبه تقرر أنك قد قرأت هذا الميثاق لتكنولوجيا الإعلام والاتصال، وأنك تتعهد بالامتثال للقواعد المذكورة فيه.

الاسم و اللقب :.....

المصلحة : .....

القسم : .....

الوظيفة : .....

بتاريخ : .....

الامضاء : .....

ملاحظة : يرجى إعادة هذه الوثيقة موقعة ومؤرخة إلى مركز الأنظمة و الشبكات.