الجمهوريـــة الجزائريـــة الديمقراطيـــة الشعبيـــة

وزارة التعليـم العالي و البحث العلمـي

جامعة زيان عاشور – الجلفـة -

المرجع الوطني للأمن المعلوماتي

R.N.S.I / 2020

ميثـــاق الأمن المعلوماتـــــي

إصدار 2022/01

تمهيـــــد

تتيح الجامعة وهياكلها للمستعملين موارد للإعلام الآلي لتمكينهم من مزاولة المهام المسندة إليهم.

إن إساءة استخدام هاته الموارد من شأنه أن يعرض للخطر أمن منظومة الإعلام الآلي للجامعة وهياكلها.

وكجزء من **تنفيذ المرجع الوطني لأمن المعلومات المطبق على القطاع** ، تقرر وضع ميثاق للأمن المعلوماتي لضمان الحد الأدنى من الأمان.

المادة 1: الغرض

الغرض من هذا الميثاق هو تحديد شروط استخدام موارد الإعلام الآلي في الجامعة وهياكلها كما يحدد قواعد السلامة التي يجب على المستعملين احترامها.

المادة 2: نطاق التطبيق

يطبق هذا الميثاق على أي شخص لديه حق الوصول الدائم أو المؤقت إلى موارد الإعلام الآلي للجامعة وهياكلها.

المادة 3: ملكية موارد الإعلام الآلي

- جميع موارد الإعلام الآلي المتاحة للمستعملين هي ملكية حصرية للجامعة وهياكلها.
- جميع البيانات المهنية المخزنة في معدات الجامعة أو التي تمر عبر شبكاتها هي ملكية حصرية للجامعة وهياكلها.

المادة 4: شروط الوصول إلى موارد الإعلام الآلي والشبكة المعلوماتية

يخضع الوصول إلى موارد وشبكات الإعلام الآلي الخاصة بالجامعة وهياكلها إلى تعريف دخول مسبق باستخدام اسم وكلمة مرور موثقة.

المادة 5: مسؤولية المستعمل

المستعمل وحده هو المسؤول عن أي استخدام لوسائل توثيق الهوية الرقمية التي توفرها له الجامعة وهياكلها.

المادة 6: حماية وسائل توثيق الهوية الرقمية

للحفاظ على وسائل توثيق الهوية الرقمية المتوفرة له، يجب على المستعمل:

- ضمان حماية وحفظ المعلومات السرية المتعلقةبالولوج لموارد الإعلام الآلي والشبكة.
- تغيير معلومات الدخول لمختلف الموارد والخدمات الرقمية إلى تغيير دوري لأرقامها السرية.
- يحظر تماما إعطاء معلومات الدخول السرية الخاصة بالمستعمل إلى طرف ثالث.

المادة 7: استخدام موارد الإعلام الآلي للجامعة وهياكلها

- لا يمكن استخدام موارد الإعلام الآلي الخاصة بالجامعة وهياكلها إلا للأغراض المهنية.
- يجب على المستخدم أن يحافظ على موارد الإعلام الآلي المتاحة له.
- لا يسمح للمستعمل بتثبيت برامج غير مرخصة على موارد الإعلام الآلي المتاحة له.
- وفي حالة حدوث خلل تقني في هذه الوسائل أو الموارد، يجب عليه إبلاغ الهيكل التقني المباشر على الفور.

المادة 8: التزامات الجامعة وهياكلها تجاه المستعملين

تقوم الجامعة وهياكلها بما يلي:

- إتاحة موارد تكنولوجيا الإعلام الآلي اللازمة للمستعمل لأداء المهام المنوطة به.
- ضمان الأداء السليم لموارد الإعلام الآلي وتوافرها.
- الحفاظ على جودة الخدمة المقدمة للمستعملين في حدود الموارد المخصصة لهم.
- إعلام المستعملين بالسياسات والإجراءات المطبقة على موارد الإعلام الآلي المعمول بها.
- تنفيذ الوسائل اللازمة لضمان سرية وسلامة الوثائق وعمليات التبادل الالكتروني للمستعملين.
- إعلام المستعملين بأن أنشطة الشبكات وأنظمة الإعلام الآلي تخضع للمراقبة الآلية.
- تحسيس المستعملين وجعلهم على دراية بالمخاطر المرتبطة بالأمن المعلوماتي.

المادة 9: التزامات المستعملين

يجب أن يلتزم المستعمل بما يلي:

- الامتثال للقوانين واللوائح المعمول بها.
- الامتثال لهذا الميثاق ومختلف إجراءات وسياسات الجامعة وهياكلها.
- تطبيق التدابير والإرشادات الخاصة بالأمن المعلوماتي بكل دقة.
- عدم استخدام حسابات الآخرين أو محاولة استخدامها.
- الإبلاغ السريع عن أي خلل تقني مشبوه أو مخاطر أمنية تقنية دون تأخير.

المادة 10: سلامة محطات العمل وحمايتها

يجب أن يتبع المستعمل تعليمات الأمان التالية بكل دقة:

- تأمين وإقفال الوصول إلى محطة العمل في حالة عدم الحضور حتى وان كان الغياب مؤقتا
- تنبيه المصالح التقنية في حالة اكتشاف جهاز جديد متصل بمحطة العمل.
- التأكد من أن محطة العمل الخاصة بالمستعمل تحتوي على برنامج مكافحة الفيروسات، وإبلاغ المصالح التقنية المعنية بأي مخاطر أو تنبيهات تقنية أمنية.
- يمنع مطلقا توصيل الأجهزة الشخصية بمحطة العمل.
- فحص كل الوسائط القابلة للإزالة المتصلة بمحطة العمل قبل أي استخدام.
- إيقاف تشغيل الأجهزة المعلوماتية أثناء فترات عدم النشاط لفترات طويلة.
- عدم التدخل بالصيانة في محطات العمل أو الشبكة (فتح الخزانات الشبكية/الوحدات المركزية ...)

القسم 11: استخدام البريد الإلكتروني المهني

توفر الجامعة وهياكلها للمستعملين حسابات بريد إلكتروني مهني وأكاديمي تسمح لهم بإرسال رسائل إلكترونية متعلقة بالعمل وتلقيها.

يمكن استخدام مراسلات العمل لأغراض العمل فقط. وتحقيقا لهذه الغاية، يحظر تماما:

- استخدامه لأغراض شخصية وغير مهنية.
- استخدامه للتسجيل على الشبكات الاجتماعية والمنتديات ومواقع الويب.
- فتح المرفقات و/أو الارتباطات التشعبية المرسلة من عناوين بريدية إلكترونية غير معروفة.
- فتح صندوق البريد المهني من الأماكن العمومية ، ولاسيما فضاءات الانترنيت العامة والتجارية.

عندما تتطلب مهام المستخدم التسجيل على الشبكات الاجتماعية أو المنتديات أو مواقع الويب، يتم تعيين عنوان بريد إلكتروني مخصص لهذا الغرض له بعد الحصول على موافقة السلطة المخولة.

يجب أن يكون المستخدم متيقظا عند استخدام رسائل البريد الإلكتروني من خلال التأكد مما يلي:

- عنوان المتلقي جيد الصياغة.
- يحق للمتلقي الوصول إلى المحتوى المرسل.
- تم إرفاق المرفقات الصحيحة بالمستند.

يحظر تماما استخدام عناوين البريد الإلكتروني الشخصية لإرسال المستندات المهنية.

المادة 12: استخدام الإنترنت

يتعهد المستعملون الذين لديهم إمكانية الوصول إلى الإنترنت بما يلي:

- أن لا تستعمل هذه الخدمة عمدا في البرامج الضارة أو الفاحشة أو الاحتيالية أو البغيضة أو الافترائية، الأغراض الإباحية أو غير المشروعة؛
- عدم تقديم معلومات تتعلق بالوظيفة أو الرتبة أو المسؤولية على الشبكات الاجتماعية.
- تجنب الاستخدام المكثف للشبكة المعلوماتية للجامعة وهياكلها مما يؤدي إلى تشبعها أكثر من اللازم.
- توخي الحذر عند تنزيل الملفات، والتأكد من فحصها باستخدام برنامج مكافحة الفيروسات.

المادة 13: الأجهزة المحمولة ووسائط التخزين

يجب على المستعمل:

- إبلاغ الإدارة فورا بأي فقدان أو سرقة لجهاز محمول أو جهاز تخزين مهني.
- تأمين الأجهزة المحمولة دائما عند عدم استخدامها.
- تعطيل **Wifi** و **htooteulB** على الأجهزة في حالة عدم احتياجهم.
- حظر رسمي على أي شخص من خارج المؤسسة لنقل المستندات في وسائط قابلة للإزالة، ويجب إجراء أي عملية تبادل للمستندات عبر البريد الإلكتروني المهني. وفي حالة ما إذا كان حجم البيانات يتطلب استخدام وسائط قابلة للإزالة، يجب أن تقوم الدوائر المختصة بتحليل هاته الوسائط قبل استخدامها.
- تشفير وترميز البيانات السرية الحساسة في أجهزة تخزين خارجية خاصة ومؤمنة.
- أثناء التنقلات العلمية أو المهنية ، يجب على المستخدمين الاحتفاظ بالأجهزة المحمولة ووسائط التخزين القابلة للإزالة معهم .

المادة 14: التدابير الأمنية الواجب تطبيقها عند السفر إلى الخارج

- يحظر استخدام الأجهزة الطرفية العامة أو المشتركة (أجهزة الكمبيوتر أو الأجهزة اللوحية)

للوصول إلى حساب البريد الإلكتروني المهني أو تطبيقات الأعمال المهنية.

- يجب على القائم بالمهمة المهنية أن يحافظ على الأجهزة المهنية معه .
- يجب على القائم بالمهمة المهنية تعطيل وظائف الاتصال اللاسلكي مثل iW- iF والبلوتوث على الأجهزة عندما لا يكون ذلك مطلوبا.
- ويجب على القائم بالمهمة المهنية حذف جميع البيانات المهنية الحساسة، غير الضرورية للمهمة، من جميع وسائط الإعلام الآلي القابلة للإزالة قبل السفر إلى الخارج.
- يجب عليه أن يبلغ المسؤول المباشر والممثل الدبلوماسي الجزائري في حالة قيام السلطات الأجنبية بتفتيش معدات الحاسوب أو الاستيلاء عليها أثناء المهمات خارج الوطن.
- يحظر استخدام المعدات التي تقدم أثناء السفر إلى الخارج لأغراض مهنية.
- ويجب أن يذكر في تقارير التربصات أو المهمات الأجهزة المرتبطة التي عرضت عليه بالخارج.

- يحظر تماما نقل الوثائق من قبل شخص أجنبي عبر وسائل تخزين قابلة للإزالة . يجب إجراء جميع عمليات تبادل الوثائق عن طريق البريد الإلكتروني فقط.
- يجب على القائم بالمهمة تغيير كلمات المرور المستخدمة أثناء المهمة.

المادة 15: نهاية العلاقة بين المستخدم والجامعة وهياكلها

عندما تنتهي العلاقة بين المستخدم والجامعة:

- يجب أن يُرجع إلى الجامعة كافة موارد الإعلام الآلي التي تم توفيرها له.
- تقوم الجامعة بحذف كافة بيانات الوصول الخاصة بالمستخدم المغادر والتي وفرتها له الجامعة وهياكلها.

القسم 16: تسيير المخاطر التقنية

في حالة وقوع مخاطر تقنية مؤثرة على الأمن بالجامعة وهياكلها سيتم:

- تجميد الوصول التقني لموارد الإعلام الآلي والشبكة، مع إشعار أو بدون إشعار، وفقا لشدة الحالة.
- عزل أو إبطال أي بيانات أو ملفات تتعارض مع الميثاق أو تعرض أمن نظم المعلومات للخطر.
- إخطار المسؤول المباشر.

المادة 17: عدم الامتثال للميثاق

يؤدي عدم الالتزام بالقواعد المنصوص عليها في هذا الميثاق إلى تحمل المستعمل لمسؤوليته ويؤدي إلى اتخاذ تدابير تأديبية تتناسب مع خطورة الحقائق التي تم التوصل إليها.

يجوز للمسؤولين التقنيين القيام بما يلي، بشرط إعلام المسؤول المباشر بذلك:

- إنذار المستعمل.
- التجميد المؤقت لوصول المستخدم لموارد الإعلام الآلي أو الشبكة.
- حذف أو عزل أي بيانات أو ملفات تتعارض مع الميثاق أو قد تعرض أمن أنظمة المعلومات للجامعة وهياكلها للخطر.

دون المساس بالجزاءات التأديبية، قد يكون انتهاك أحكام هذا الميثاق موضوع إجراءات قانونية.

المادة 18: بدء التطبيق

يبدأ تطبيق وإلزام هذا الميثاق بمجرد أن يوقع عليه المستخدم.

إن أي رفض للتوقيع يمنع المستخدم من الوصول إلى موارد المعلوماتية الخاصة بالجامعة وهياكلها.