ميثاق أمن تكنولوجيا المعلومات

الديباجة

سخرت المؤسسة لمجمل المستخدمين وسائل تكنولوجيا المعلومات بغية تمكينهم من إنجاز المهام المنوطة بهم، بيد ان سوء استخدام هذه الوسائل قد يرفع من درجة المخاطر التي من شأنها الإضرار بأمن المنظومة المعلوماتية للمؤسسة.

وعليه فقد تقرر إعداد ميثاق "الأمن المعلوماتي" المدرج في إطار تطبيق المرجع الوطني للأمن المعلوماتي بغية ضمان الحد الادنى من الأمن.

مفاهيم اصطلاحية:

- **المستعمل:** وفق أحكام هذا الميثاق يعد مستعملا أيّ شخص مخوّل للوصول إلى أدوات تكنولوجيا المعلومات بالمركز الجامعي ووسائل الاتصال واستخدامها وهم الموظّفون الدائمون أو المتعاقدون، والطّلاب، والمتدخّلون الخارجيون، والزائرون، والمدعوون.

- **CSSI**: خلية أمن نظام المعلومات.

- **CSRICTED:** مركز أنظمة المعلومات والشبكات ،والاتصالات والتعليم عن بعد.

- **BSN:** مكتب استراتيجية الرقمنة وهو هيئة استشارية تعنى بعملية مرافقة عملية التجسيد الميداني لعملية الرقمنة على مستوى المركز الجامعي ، وتنفيذ أحكام وقواعد هذا الميثاق.

-**CATI** : مركز الدعم التكنولوجي والابتكار وهو الهيئة الوحيدة والرئيسية المعنية بعملية تسجيل براءات الاختراع وحماية الأفكار المبتكرة للطلبة والباحثين.

- **INAPI** : المعهد الوطني الجزائري للملكية الصناعية.

-**ONDA** : الديوان الوطني لحقوق المؤلف.

- **ARN** : شبكة البحث الأكاديمي.

- **الموارد المعلوماتية**: تتكون بشكل خاص من موارد المعلومات وموزع الخدمات ومحطات العمل والشبكات الداخلية والخارجية للمركز الجامعي ومعدات الاتصالات السلكية واللاسلكية والبنى التحتية لربط الشبكة وشبكة ARN والميكروفونات وأجهزة الكمبيوتر في الأقسام والمخابر ووحدات البحث، بالإضافة إلى مجمع البرامج، قاعدة البيانات والحسابات المؤسسية، إجراءات المراقبة، التطبيقات النقّالة، المنتجات متعددة الدعائم أو الملحقات المخصصة لتشغيلها.

المخاطر: تشير إلى المخاطر التي تتطلب الامتثال لقواعد معينة للسلامة وحسن السلوك. يمكن أن يكون لتهور المستعمل أو إهماله أو كيده عواقب وخيمة مثل تحمل المسؤولية المدنية و / أو الجنائية وكذلك مسؤولية المؤسسة.

البيانات ذات الطبيعة الشخصية: تقابل أي معلومات تتعلق بشخص طبيعي تم تحديده أو يمكن تحديد هويته، بالرجوع إلى رقم تعريف أو عنصر أو أكثر خاص به، وفق احكام القانون 18-07 المؤرخ في 2018/06/10 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

المادة الأولى: القواعد المبدئية

يزود المركز الجامعي الشريف بوشوشة موظفيه ومستعمليه بأدوات تقنية المعلومات ووسائل الاتصال لتمكينهم من إنجاز المهام الموكلة إليهم.

يندرج هذا النص ضمن الإطار التشريعي والتنظيمي المعمول به فيما يتعلق بحماية البيانات، واستخدام البرمجيات وحقوق والتزامات مستعملي الخدمات الرقمية .لاسيما ما نصت عليه أحكام الأمر 03-05 المؤرخ في 2003/07/19 المتعلق بحقوق المؤلف والحقوق المجاورة.

المادة 02: الأهداف

يحدّد هذا الميثاق قواعد الأمان والشروط العامة وأحكام استخدام الموارد المعلوماتية ووسائل الاتصال بالمركز الجامعي.

والغرض منه هو توعية المستعملين بالمخاطر المرتبطة باستخدام هذه الموارد من حيث سلامة وسرية المعلومات التي تتّم معالجتها. كما يصف العقوبات المفروضة في حالة عدم الامتثال لقواعد السلامة هذه، ويذكر بالنصوص المرجعية الرئيسية.

يتم توزيع الميثاق على جميع المستعملين بأيّ وسيلة وفي كل مرّة يتم إصدار نسخة جديدة. على هذا النحو، كما يتم نشره على الموقع الرسمي للمركز، مع إيصاله بصفة آلية لجميع الوافدين الجدد على المركز.

المادة 03: مجال التطبيق

ينطبق هذا الميثاق على أي شخص لديه وصول دائم أو مؤقت إلى موارد تكنولوجيا المعلومات الخاصة بالمركز الجامعي.

المادة 04: حول ملكية الموارد المعلوماتية

جميع الموارد المعلوماتية المتاحة للمستعملين هي ملكية حصرية للمركز الجامعي.

تعد كل البيانات المخزنة في الأجهزة أو المنقولة عبر شبكات موارد تكنولوجيا المعلومات ملكية خاصة للمركز الجامعي.

المادة 05: شروط الوصول إلى الموارد والشبكة المعلوماتية

تخضع كل عملية ولوج الى موارد او شبكة تكنولوجيا المعلومات الى إجراء إثبات الهوية المسبق.

المادة 06: مسؤولية المستخدم

المستخدم هو المسؤول الوحيد عن أي استخدام محلي أو عن بعد للموارد المعلوماتية المتاحة له من قبل المركز، وكذلك عن جميع المعلومات التي يتيحها للغير عبر الموارد المعلوماتية الخاصة بالمركز.

المادة 07: المحافظة على وسائل إثبات الهوية

سعيا للمحافظة على وسائل إثبات الهوية المتاحة يستوجب على المستخدم ما يلي:

* الحرص على حفظ وحماية سرية المعلومات الخاصة بإجراء إثبات الهوية.
* الحرص على التغيير الدوري للمعلومات السرية الخاصة بإثبات الهوية.
* يمنع منعا باتا إطلاع أي شخص آخر على سرية المعلومات الخاصة بإثبات الهوية.

* قطع الاتصال في نهاية كل فترة عمل.
* عدم القيام بإجراء أي تغييرات على البيانات دون الحصول على موافقة مسبقة من مسؤول CSSI.
* عدم القيام بتثبيت أي برنامج بدون موافقة مسؤول CSSI.
* عدم القيام بتوصيل معدات الشبكة دون موافقة مسؤول CSSI.
* التأكد من تفعيل برنامج مكافحة الفيروسات وتحديثه دوريًا على محطة عمله.
* عدم القيام بأي عملية من شأنها تغيير أو مقاطعة التشغيل العادي للنظام المعلوماتي للمركز.
* يُمنع منعًا باتًا إبلاغ معلومات المصادقة السرية الخاصة به إلى جهات خارجية.

المادة 08: استخدام موارد تكنولوجيا المعلومات

لا يجوز استخدام تكنولوجيا المعلومات الخاصة بالمركز الجامعي إلا لأغراض مهنية بحتة.

يجب على المستعمل الحفاظ على موارد تكنولوجيا المعلومات والوسائل المتاحة له.

لا يسمح للمستخدم تثبيت أو تشغيل أي تطبيقات أو برامج على وسائل وموارد تكنولوجيا المعلومات الموضوعة تحت تصرفه.

كل مستخدم مسؤول عن الحسابات الخاصة به في موارد تكنولوجيا المعلومات، ويتحمل تبعات ما يتم نشره بواسطة هذا الحساب

وفي حالة حدوث أي خلل على مستوى هذه الوسائل أو الموارد، يجب عليه إبلاغ الهيكل المسؤول عن الصيانة بصفة فورية.

المادة 09: التزامات المركز الجامعي تجاه المستخدمين

يلتزم المركز الجامعي بما يلي:

- توفير فضاء افتراضي تعليمي مؤمن ومحمي على مستوى الموقع الرسمي للمركز الجامعي.

- تسخير موارد تكنولوجيا المعلومات اللازمة لصالح المستخدمين لإنجاز المهام المنوطة بهم.
- ضمان توفير وحسن أداء موارد تكنولوجيا المعلومات.
- ضمان جودة الخدمة المقدمة للمستخدمين في حدود الموارد المخصصة لذلك.
- إعلام المستخدمين بالإجراءات والسياسات المطبقة في مجال استخدام موارد تكنولوجيا المعلومات.
- توفير الوسائل اللازمة لضمان سرية وسلامة المستندات والتبادلات الإلكترونية بين المستخدمين.
- إعلام المستخدمين بأن الأنشطة على الشبكة والأنظمة تخضع لنظام المراقبة الآلية
- توعية المستخدمين بالمخاطر المتعلقة بأمن تكنولوجيا المعلومات.

المادة *10*: التزامات المستخدم

يجب على المستخدم القيام بما يلي:

- احترام القوانين واللوائح سارية المفعول.
- إلزامية احترام بنود هذا الميثاق و مختلف الإجراءات والسياسات الخاصة بالمركز الجامعي.
- إلزامية التطبيق الدقيق للإجراءات والتوصيات المتعلقة بالأمن المعلوماتي الخاصة بالمركز الجامعي.
- منع استخدام أو محاولة استخدام حسابات أي شخص آخر.
- الإبلاغ الفوري عن اي عمل مشبوه أو أي حدث يمس بأمن المنظومة المعلوماتية.

المادة *11*: ما يتعلق بالمراسلات الإلكترونية المهنية

يوفر المركز الجامعي لمستخدميه حسابات البريد الإلكتروني التي تتيح لهم تلقي وإرسال رسائل الكترونية ذات طابع مهني،

لا يسمح باستخدام البريد الالكتروني المهني الا لأغراض مهنية بحتة وعليه يمنع منعا باتا ما يلي:

- استخدامه لأغراض شخصية أو حزبية.
- استخدامه للتسجيل في الشبكات الاجتماعية والمنتديات والمواقع الإلكترونية.
- فتح المرفقات أو الروابط المرسلة من عناوين بريدية إلكترونية مجهولة.
- فتح صندوق البريد الإلكتروني المهني عبر المرافق العامة المتاحة لخدمة الأنترنت، لاسيما مقاهي الأنترنت.
- استخدام عناوين البريد الإلكتروني الشخصية لإرسال المستندات المهنية.

عند الحاجة يرخص للمستخدم التسجيل على مواقع التواصل الاجتماعي والمنتديات والشبكات العنكبوتية عن طريق بريد إلكتروني مخصص لهذا الغرض بعد موافقة الجهة المؤهلة لذلك.

- على المستخدم توخي الحذر عند استخدام الرسائل الإلكترونية وذلك من خلال التأكد مما يلي:

* صحة بيان عنوان المرسل إليه
* أن يكون المتلقي مخول للاطلاع على محتوى الرسالة الإلكترونية
* إرفاق الوثائق بالمرفقات الخاصة بها.

المادة 12: استخدام الانترنت:

يلتزم مستخدمو خدمة الأنترنت بما يلي:

- عدم استخدام خدمة الأنترنت لأغراض مضرة وفاحشة ومدلسة ومبغضة وتشهيرية وإباحية وغير قانونية.
- عدم نشر معلومات متعلقة بمهنته ورتبته ومنصبه عبر شبكات التواصل الاجتماعي.
- تجنب تحميل الشبكة فوق طاقة استيعابها.
- توخي الحذر أثناء تحميل الملفات والتأكد من فحصها عن طريق برنامج مكافحة الفيروسات.

المادة 13: أمن وحماية أجهزة الكمبيوتر

يستوجب على المستخدم أن يحترم بدقة تعليمات الأمن التالية:

- الحرص على تفعيل وضع قفل الأجهزة في حالة الغياب ولو كان بشكل مؤقت.
- إبلاغ المصالح التقنية في حالة اكتشاف اتصال أي جهاز جديد بجهاز الكمبيوتر الخاص بك.
- التأكد من أن جهازك يتوفر على برنامج مكافحة الفيروسات وإبلاغ المصالح المعنية عن أي تنبيه أمني.
- اجتناب توصيل الأجهزة الخاصة بجهاز الكمبيوتر الخاص بالعمل.
- مسح كل الوسائط القابلة للإزالة قبل استخدامها على أجهزة الكمبيوتر.
- إيقاف تشغيل أجهزة الكمبيوتر أثناء فترات التوقف عن العمل الطويلة ليلا وعطلة نهاية الاسبوع والعطل السنوية.
- تجنب محاولة إصلاح الأجهزة كفتح الوحدات المركزية وما الى ذلك....

المادة 14: الأجهزة المحمولة ودعائم التخزين

يجب على المستخدم ما يلي:

- تبليغ المسؤول المباشر فورا عن أي ضياع أو سرقة طالت الجهاز المحمول أو واسطة التخزين الخاصة بالعمل.
- الحرص على تفعيل خاصية "القفل" للأجهزة في حالة عدم استخدامها.
- عدم تشغيل خاصيتي البلوتوث والاتصال اللاسلكي للأجهزة عند عدم الحاجة لذلك.
- يمنع منعا باتا على الأشخاص الغرباء عن المؤسسة نقل الملفات عبر الوسائط الخارجية، وعليه فإن كل تبادل للملفات يتم عن طريق البريد الإلكتروني حصرا.
- وفي حالة ما إذا كان حجم الملفات يتطلب النقل عبر وسائط التخزين الخارجية، فإنه يجب فحصها من طرف الجهات المخولة لذلك.
- تشفير البيانات السرية الموجودة في الأجهزة المحمولة ودعائم التخزين.
- يجب على المستخدم الاحتفاظ بأجهزته المحمولة ووسائط التخزين القابلة للإزالة معه أثناء تنقلاته المهنية.

المادة 15: تطبيق الإجراءات الأمنية عند السفر إلى الخارج.

- يحظر استخدام أي جهاز طرفي (كمبيوتر أو لوحة إلكترونية) الموجهة للاستخدام العام أو المشترك للاتصال بالبريد الإلكتروني المهني أو التطبيقات المتعلقة بإدارة المؤسسة.
- يجب على المكلف بأداء مهمة أن يحتفظ بالأجهزة الطرفية المهنية ووسائط التخزين معه بصفة دائمة.
- يجب على المكلف بأداء مهمة إيقاف تشغيل وظائف الاتصال اللاسلكية (البلوتوث وخاصية الاتصال اللاسلكي) للأجهزة عند عدم الحاجة لذلك.
- يجب حذف كل البيانات المهنية ذات الأهمية غير المعنية بالمهمة من على الوسائط القابلة للإزالة قبل التوجه لأداء أي مهمة في الخارج.
- يجب إبلاغ المسؤولين المباشرين أو ممثلي الدبلوماسية الجزائرية في حالة حجز أو تفتيش أجهزة تكنولوجيا المعلومات من طرف السلطات الأجنبية أثناء القيام بمهام خارج الوطن.
- يحظر استخدام لأجل أغراض مهنية أي جهاز تم تسخيره أثناء التنقل للخارج.
- يجب أن يذكر في التقارير الخاصة بالمهمة قائمة كل الأجهزة المسخرة التي تم توصيلها أثناء التنقل.
- يمنع منعا باتا تحويل أي ملفات عن طريق أي شخص غريب بواسطة الوسائط القابلة للإزالة.

وعليه فكل التبادلات تتم حصريا عبر البريد الإلكتروني.

- يتوجب على المكلف بمهمة في الخارج تغيير كلمات السر أثناء القيام بمهمته.

المادة 16: حماية المصنفات الرقمية التابعة للمركز الجامعي

في إطار احترام قواعد وأحكام الأمر 03-05 المؤرخ في 2003/07/19 المتعلق بحقوق المؤلف والحقوق المجاورة، وكذا أحكام القرار الوزاري رقم 1082 الصادر عن وزارة التعليم العالي الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية فإن المصنفات الرقمية التي يملكها المركز الجامعي مشمولة بالحماية القانونية والرقابة اللازمتين والموضوعة تحت مسمى **قاعدة بيانات الأعمال المنجزة** من قبل الطلبة والأساتذة.

تعتبر المصنفات الرقمية التي تندرج ضمن هذا الإطار على وجه الخصوص ما يلي:

- كل المنشورات العلمية أو البيداغوجية التي ينتجها الأساتذة الجامعيون التابعون للمركز الجامعي والموضوعة على مستوى الموقع الرسمي للمركز الجامعي.
- مذكرات التخرج ليسانس – ماستر –دكتوراه التي ينتجها طلبة المركز الجامعي.
- مذكرات التخرج الخاصة بشهادة -مؤسسة ناشئة وشهادة-براءة الاختراع، والتي تعمل CATIبالتنسيق مع هيئتي INAPIوONDA، بالإسراع في عملية التسجيل القانوني والحماية اللازمة لهذه المشاريع مع متابعة وضعية حقوق الملكية الفكرية والصناعية للطلبة والباحثين، وتذليل كافة الصعوبات التي تطرأ على هذه المؤسسات عبر كل مراحلها.
- أعمال الملتقيات الدولية والوطنية المنشورة على مستوى المركز الجامعي.
- الدروس ومختلف الأعمال البيداغوجية الموضوعة من طرف الأساتذة على مستوى المنصة التعليمية الافتراضية للمركز الجامعي.
- تقارير التربصات الميدانية التي يجريها الأساتذة والطلبة في الخارج.
- مشاريع البحث.

المادة 17: آليات حماية المصنفات الرقمية التابعة للمركز الجامعي

تطبيقا لأحكام المادة 06 من القرار الوزاري رقم 1082 والتي تلزم كل مؤسسات التعليم العالي ومؤسسات البحث باتخاذ تدابير الرقابة، فإنه يتعين ما يلي:

- ضمان عملية الرقابة على قاعدة بيانات الأعمال المنجزة من قبل الطلبة والأساتذة.
- التحيين الدوري لقاعدة البيانات الرقمية لأسماء الأساتذة التابعين للمركز الجامعي حسب شعبهم وتخصصاتهم، كما تشمل سيرهم الذاتية، ومجالات اهتماماهم العلمية والبحثية، للاستعانة بخبراتهم من أجل تقييم أعمال وأنشطة البحث العلمي.

- تفعيل دور البرمجيات المعلوماتية الكاشفة للسرقات العلمية باللغة العربية واللغات الأجنبية بما فيها البرمجيات المجانية المتوفرة في شبكة الانترنت، وغيرها من البرمجيات المتوفرة، مع تفضيل برمجية معلوماتية جزائرية أو محلية عند الاقتضاء.

المادة 18: فك الارتباط بين المستخدم والمركز الجامعي او بتغيير المهمة

عندما تنتهي العلاقة بين المستخدم وإدارة المركز الجامعي، يجب على المستخدم إعادة جميع الموارد المعلوماتية مع الأجهزة المتاحة التي تم تسخيرها سلفا.

تزيل إدارة المركز الجامعي أية عملية وصول للمستخدم السابق إلى الموارد المعلوماتية التي كانت متاحة له.

في حالة تغيير المهمة، يجب على المستعمل إعادة جميع الموارد المعلوماتية التي كانت متاحة له إلى رئيسه المباشر، كما يقوم هذا الأخير بإبلاغ الإدارة المعنية بهذا التغيير.

المادة 19: إدارة العوارض

في حالة وقوع أي عارض من شأنه الإضرار بالأمن الإلكتروني، يتوجب ما يلي:

- قطع الاتصال عن المستخدم ،مع أو بدون إشعار بحسب خطورة الوضع.
- عزل أو تحييد بصفة مؤقتة أي ملفات أو بيانات تتعارض مع بنود هذا الميثاق أو من شأنها أن تعرض منظومة الأمن المعلوماتي للخطر .
- إخطار المسؤول المباشر .

المادة 20: الأحكام المتعلقة بمخالفة قواعد ميثاق البيئة الرقمية

من المرجح أن يؤدي عدم الامتثال للقوانين المحددة في هذا الميثاق إلى تحميل المستخدم المسؤولية مما قد يؤدي الى اتخاذ تدابير تأديبية ضده، تتناسب مع خطورة الوقائع المرتكبة.

رهنا بإخطار المسؤول المباشر. يمكن للمسؤولين على أمن تكنولوجيا المعلومات التصرف كما يلي:

- إخطار المستخدم.
- حضر أو تقييد اتصال المستخدم بصفة مؤقتة.
- حذف أو تقييد او عزل كل البيانات أو الملفات التي تتعارض مع بنود هذا الميثاق والتي من شأنها أن تعرض الأمن المعلوماتي للخطر.
- يخضع كل مخالف لأحكام هذا الميثاق الى المتابعة القضائية دون الإخلال بالعقوبات الانضباطية المتخذة سلفا.

المادة 21: الأحكام الختامية (بدء السريان وأحكام التعديل)

يدخل هذا الميثاق حيز التنفيذ بمجرد توقيعه من طرف مدير المركز الجامعي وتوقيعه من طرف المستخدم وفي حالة رفض المستخدم التوقيع على الميثاق يمنع بموجبه المستخدم من الاتصال بموارد تكنولوجيا المعلومات الخاصة بالمؤسسة.

تخضع أحكام هذا الميثاق إلى التعديل كلما دعت الضرورة إلى ذلك، ويتم تبليغ كافة المعنيين بهذه التعديلات عبر الموقع الرسمي للمركز الجامعي.

يأتي طلب التعديل من طرف كل من:

- مدير المركز الجامعي
- مسؤول CSSI

مدير المركز الجامعي

مدير المركز الجامعي آفلو

إمضاء: عبد الكريم طهاري