



ميثاق المعلوماتية الخاص بجامعة محمد الشريف مساعدي سوق أهراس



تضع جامعة محمد الشريف مساعدي سوق أهراس تحت تصرف المستخدمين (الأساتذة، الموظفين، الطلبة والزائرين) وسائل معلوماتية للسماح لهم بإنجاز المهام المسندة إليهم. إن سوء استخدام هذه الوسائل يزيد من مخاطر المساس بأمن أنظمة المعلومات الخاصة بالجامعة.

لقد تقرر إصدار ميثاق المعلوماتية هذا في إطار تطبيق المرجع الوطني للأمن المعلوماتي لضمان حد أدنى من الأمن.

المادة 1 : الهدف

يهدف الميثاق إلى التعريف بشروط وكيفيات استعمال الموارد المعلوماتية لجامعة محمد الشريف مساعدي سوق أهراس وقواعد الأمن التي يتوجب على المستخدمين احترامها.

المادة 2 : مجال التطبيق

ينطبق الميثاق الحالي على كل شخص بإمكانه الوصول بشكل دائم أو مؤقت إلى الموارد المعلوماتية لجامعة محمد الشريف مساعدي سوق أهراس.

المادة 3 : ملكية الموارد المعلوماتية

- جميع الموارد المادية الموضوعة تحت تصرف المستخدمين (من حواسيب، شبكات، عتاد وأجهزة مختلفة) تُعد مملوكة حصريا لجامعة محمد الشريف مساعدي سوق أهراس، ويجب المحافظة عليها؛

- كل الوثائق التي تُنجز تحت ركن البيانات التي تُنتج باسم الجامعة أو لمصلحتها تُعد مملوكة حصريا لها مع مراعاة النصوص القانونية والتنظيمية التي تحمي حقوق الملكية الفكرية والأدبية.

المادة 4 : شروط الدخول إلى الموارد المعلوماتية والشبكة

جميع الموارد وشبكات المعلوماتية الخاصة بجامعة محمد الشريف مساعدي سوق أهراس تخضع لإجراء التصديق المسبق الذي يشمل ولا يقتصر على اسم حساب المستخدم وكلمة سره.

المادة 5 : مسؤولية المستخدم

يُعد المستخدم مسؤولا لوحده عن كل استعمال لوسائل التصديق الموضوعة تحت تصرفه من قبل الجامعة.

المادة 6 : حماية وسائل التصديق

من أجل حماية وسائل التصديق الموضوعة تحت تصرف المستخدم يجب على هذا الأخير:

- السهر على حماية معلوماته السرية الخاصة بالتصديق والحفاظ عليها؛
- تغيير معلومات السرية الخاصة بالتصديق بشكل دوري؛
- يُمنع منعا باتا إعطاء المعلومات السرية الخاصة بالتصديق للغير.

المادة 7 : استعمال الموارد المعلوماتية

- يُمنع منعا باتا استعمال الموارد المعلوماتية الخاصة بالجامعة إلا لأهداف مهنية؛
- على المستخدم الحفاظ على الموارد المعلوماتية الموضوعة تحت تصرفه؛
- لا يُسمح للمستخدم بتثبيت برامج أو تطبيقات على الموارد المعلوماتية الموضوعة تحت تصرفه دون إذن مُسبق من مديري هذه الموارد؛

- في حالة حدوث خلل في هذه الموارد على المستخدم إعلام المصالح المكلفة بالصيانة فورا.

المادة 08 : التزامات الجامعة اتجاه المستخدم.

يلتزم الجامعة بـ:

أ- أن تضع تحت تصرف المستخدم الموارد المعلوماتية الضرورية لتنفيذ المهام المسندة إليه

ب- ضمان التشغيل الحسن للموارد المعلوماتية وتوفيرها؛

ج- الحفاظ على جودة الخدمة المقدمة للمستخدمين في حدود الإمكانيات المتاحة؛

- إعلام المستخدمين بالإجراءات والسياسات المطبقة في مجال الموارد المعلوماتية؛
- العمل على توفير الوسائل الضرورية لضمان حرية وسلامة وخصوصية الوثائق والتبادلات الإلكترونية للمستخدمين؛
- إعلام المستخدمين بأن الأنشطة على الشبكة والأنظمة خاضعة للرقابة الآلية؛
- تحسيس المستخدمين بالمخاطر المرتبطة بالأمن المعلوماتي.

المادة 09 : التزام المستخدم

يلتزم المستخدم بـ:

- احترام القوانين والأنظمة سارية المفعول؛
- احترام هذا الميثاق وكذلك مختلف الإجراءات وسياسات الجامعة؛
- التطبيق الحرفي للتدابير والتوصيات المتعلقة بأمن المعلوماتية الخاصة بالجامعة؛
- عدم استخدام أو محاولة استخدام حسابات الآخرين؛
- التبليغ فوراً عن كل نشاط مشبوه أو حادث يمس بالأمن المعلوماتي.

المادة 10 : تأمين حواسيب العمل وحمايتها

يجب على المستخدم احترام تعليمات الأمان التالية بدقة:

- غلق حاسوب العمل في حالة الغياب، ولو لفترة قصيرة؛
- تنبيه المصلحة التقنية المختصة في حالة اكتشاف معدات جديدة متصلة بحاسوب العمل؛

- التأكد من تشغيل برنامج مكافحة فيروسات على حاسوب العمل، وإبلاغ الجهات المعنية بأي تنبيه أمني؛
- يمنع منعاً باتاً توصيل المعدات الشخصية للمستخدم بحواسيب العمل؛
- فحص جميع الوسائط المحمولة (مثل مفتاح يو أس بي (USB) عند ربطها بالحاسوب قبل الاستخدام؛
- إيقاف تشغيل الحواسيب خلال فترات الخمول الطويلة (الليل، عطلة نهاية الأسبوع، العطلة السنوية...)
- يمنع التدخل الشخصي لفتح الأجهزة (فتح الوحدات المركزية للحواسيب (...)).

المادة 11 : استخدام البريد الإلكتروني المهني

توفر جامعة محمد الشريف مساعديّة سوق أهراس للمستخدمين حسابات بريدية إلكترونية لغرض استعمالها في إرسال واستقبال الرسائل الإلكترونية ذات الطبيعة المهنية.

لا يستخدم البريد الإلكتروني المهني إلا لأغراض العمل، وتحقيقاً لهذه الغاية يمنع منعاً باتاً ما يلي:

- استخدامه لأغراض شخصية أو أغراض أخرى غير مهنية؛
 - استخدامه للتسجيل ضمن مواقع التواصل الاجتماعي، المنتديات أو مختلف المواقع الإلكترونية غير المهنية؛
 - فتح المرفقات أو روابط الويب المرسلّة من عناوين بريد إلكتروني غير معروفة؛
 - الدخول على البريد الإلكتروني المهني في المساحات التي تتوفر على أنترنت مفتوحة بما في ذلك مقاهي الإنترنت.
- عندما تتطلب مهام المستخدم التسجيل ضمن مواقع التواصل الاجتماعي أو المنتديات أو مواقع ويب أخرى، سيتم إنشاء عنوان بريد إلكتروني خاص لهذا الغرض بعد الحصول على الموافقة من الجهة المخولة.
- يجب على المستخدم أخذ الحيطة والحذر عند استخدام الرسائل الإلكترونية عبر بريده المهني والتأكد من:

- صياغة عنوان المرسل إليه بشكل جيد؛
 - التأكد من أن المرسل إليه له صلاحية الوصول إلى المحتوى؛
 - التأكد من وضع المرفقات الصحيحة.
- يمنع منعاً باتاً استخدام عناوين البريد الإلكتروني الشخصية لإرسال الوثائق المهنية؛

المادة 12 : استخدام الإنترنت

يتعهد المستخدمون الذين لديهم وصول إلى الإنترنت بـ:

- عدم الاستخدام العمدي للإنترنت في أعمال التحايل، التشهير، نشر الكراهية، الدخول إلى المواقع الإباحية أو أي استعمال



- عدم نشر المعلومات المتعلقة بالوظيفة، الرتبة أو المسؤولية المتقلدة عبر مواقع التواصل الاجتماعي؛

- عدم الاستخدام التعسفي لشبكة الانترنت الخاصة بالجامعة كتحميل المحتوى الترفيهي باستعمال التورنت Torrent وغيره من

الوسائل؛

- توخي الحذر عند تنزيل الملفات، مع وجوب فحصها باستخدام برنامج مكافحة فيروسات قبل فتحها.

المادة 13 : مسؤولية المستخدم تجاه الأجهزة المحمولة ووسائل التخزين

يجب على المستخدم:

- تبليغ المسؤول المباشر فوراً بأي فقدان أو سرقة لجهاز محمول أو وسيط تخزين مهيئ؛

- ضرورة غلق الأجهزة المحمولة عندما لا تكون قيد الاستخدام؛

- ضرورة تعطيل وظائف الشبكات اللاسلكية مثل واي فاي Wi-Fi وبلوتوث Bluetooth للأجهزة عند عدم الحاجة

إليها؛

- منع أي شخص خارج الجامعة من نقل الوثائق عن طريق وسائط محمولة. أي تبادل للوثائق يجب أن يتم عن طريق البريد

الإلكتروني. إذا كان حجم البيانات يتطلب استخدام وسائط محمولة، يجب فحص هذه الأخيرة من قبل المصالح المختصة قبل

أي استخدام؛

- تشفير البيانات السرية الموضوعة في الأجهزة المحمولة ووسائل التخزين؛

- عند التنقل في سفريات خاصة بالعمل، يجب على المستخدم الاحتفاظ بالأجهزة ووسائل التخزين المحمولة معه شخصياً.

المادة 14 : التدابير الأمنية الواجب تطبيقها عند السفر إلى الخارج

- يحظر استخدام الأجهزة الطرفية (الحواسيب أو الأجهزة اللوحية) العامة أو المشتركة للوصول إلى حساب البريد الإلكتروني المهني أو التطبيقات الخاصة بالعمل؛
- يجب على المكلف بالمهمة أن يحتفظ معه في جميع الأوقات بالأجهزة المهنية وكذلك وسائط التخزين؛
- يجب على المكلف بالمهمة تعطيل وظائف الاتصال اللاسلكي مثل واي فاي Wi-Fi وبلوتوث Bluetooth للأجهزة عند عدم الحاجة إليها؛
- يجب على المكلف بالمهمة حذف جميع البيانات والمعطيات المهنية الحساسة، غير الضرورية لعمله أثناء السفر، من جميع الوسائط المحمولة قبل أي تنقل إلى الخارج؛
- يجب على المكلف بمهمة إبلاغ المسؤول المباشر والممثل الدبلوماسي الجزائري في حالة التفتيش أو مصادرة معدات الحاسوب من قبل السلطات الأجنبية أثناء البعثات إلى الخارج؛
- يُمنع استخدام الأجهزة المهداة من طرف آخر أثناء السفر إلى الخارج لأغراض مهنية؛
- يجب ذكر قائمة الأجهزة المهداة من طرف آخر أثناء السفر في تقرير المهمة؛
- يمنع منعاً باتاً على الأجنبي نقل الوثائق عبر وسائط التخزين المحمولة، ويجب أن يتم أي تبادل للوثائق حصرياً عن طريق البريد الإلكتروني؛
- يجب على المكلف بالمهمة تغيير كلمات المرور المستخدمة عند سفره.

المادة 15 : انتهاء علاقة العمل بين المستخدم والجامعة

- عندما تنتهي العلاقة بين الجامعة والمستخدم، يجب على هذا الأخير إعادة جميع الأجهزة المعلوماتية الموفرة له؛
- تقوم الجامعة بتعطيل كل وسائل الدخول للموارد المعلوماتية الممنوحة للمستخدم.
- في حالة الحسابات غير الإسمية المرتبطة بالمنصب (مثلاً رئيس قسم، رئيس مصلحة...)، يُمنع حذف محتوى الحساب.

المادة 16 : التعامل مع الحوادث الطارئة

في حالة وقوع حادث قد يؤثر على السلامة يجوز للجامعة:

- فك الارتباط المستخدم مع أو بدون إشعار وذلك حسب خطورة الحادث؛
- العزل النهائي أو التحييد المؤقت لأي بيانات أو ملفات تتعارض مع هذا الميثاق أو من شأنها أن تُعرض أمن أنظمة معلومات الجامعة للخطر؛
- إخطار المسؤول المباشر.

المادة 17 : عدم احترام ميثاق الأمن المعلوماتي للجامعة

يؤدي عدم الامتثال للقواعد المحددة في هذا الميثاق إلى تحميل المستخدم المسؤولية عن أفعاله واتخاذ تدابير تأديبية ضده تتناسب مع خطورة الوقائع الملاحظة.

تحت شرط إبلاغ المسؤول المباشر، يمكن للمسؤولين عن أمن المعلومات:

- تحذير المستخدم؛
- التقييد أو السحب المؤقت لمفاتيح الدخول الخاصة بالمستخدم.
- حذف أو ضغط أو عزل أي بيانات أو ملفات تتعارض مع الميثاق أو من شأنها أن تُعرض أمن أنظمة المعلومات للخطر.
- مع عدم الإخلال بالعقوبات التأديبية، يمكن أن يتعرض الشخص المخالف لأحكام هذا الميثاق للإجراءات القضائية السارية المفعول.

المادة 18 : الدخول حيز النفاذ

يدخل هذا الميثاق حيز التنفيذ بمجرد توقيعه من قبل المستخدم (التوقيع على التعهد والالتزام على ميثاق المعلوماتية الملحق).
أي رفض للتوقيع يحرم المستخدم من استعمال الموارد المعلوماتية الخاصة بالجامعة.

المادة 19 : المبادئ والنصوص القانونية المرجعية المطبقة

- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، المصادق عليها بموجب المرسوم الرئاسي رقم 252-14 المؤرخ في 13 ذي القعدة عام 1435 الموافق 8 سبتمبر سنة 2014.

- الأمر 156-66 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، المتضمن قانون العقوبات، المعدل والمتمم.

- الأمر 155-66 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، المتضمن قانون الإجراءات الجزائية المعدل

- الأمر رقم 03-05 المؤرخ في 19 جمادى الأولى عام 1424 الموافق 19 يوليو سنة 2003، الذي يتعلق بحقوق المؤلف والحقوق المجاورة.

- الأمر رقم 21-09 المؤرخ في 27 شوال عام 1442 الموافق 08 يونيو سنة 2021، الذي يتعلق بحماية المعلومات والوثائق الإدارية.

- القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 05 غشت 2009، الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

- القانون رقم 15-04 المؤرخ في 11 ربيع الثاني عام 1436 الموافق أول فبراير سنة 2015، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني.

- القانون رقم 18-04 المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية.

- القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، الذي يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

- المرسوم التنفيذي رقم 09-410 المؤرخ في 23 ذي الحجة عام 1430 الموافق 10 ديسمبر 2009، الذي يحدد قواعد الأمن المطبقة على النشاطات المنصبة على التجهيزات الحساسة.

- المرسوم التنفيذي رقم 61-16 المؤرخ في 2 جمادى الأولى عام 1437 الموافق 11 فبراير سنة 2016، الذي يعدّل ويتمم المرسوم التنفيذي رقم 09-410 المؤرخ في 23 ذي الحجة عام 1430 الموافق 10 ديسمبر سنة 2009، الذي يحدد

قواعد الأمن المطبقة على النشاطات المنصبة على التجهيزات الحساسة.

- المرسوم التنفيذي رقم 134-16 المؤرخ في 17 رجب عام 1437 الموافق 25 أبريل سنة 2016، الذي يحدد تنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الإلكتروني وسيرها ومهامها.
- المرسوم التنفيذي رقم 135-16 المؤرخ في 17 رجب عام 1437 الموافق 25 أبريل سنة 2016، الذي يحدد طبيعة السلطة الحكومية للتصديق الإلكتروني وتشكيلها وتنظيمها وسيرها.





مُحلق : تعهد والتزام بميثاق المعلوماتية لجامعة محمد الشريف مساعديّة سوق أهراس

أنا الممضي(ة) أسفله ،

الاسم واللقب :

المولود(ة) بتاريخ : في :

الصفة : أستاذ(ة) موظف(ة) طالب(ة) زائر(ة))

الوظيفة \ المنصب النوعي (إن وجد للأساتذة والموظفين) :

أو رقم التسجيل للطلبة :

أقر بأنني اطلعت على ميثاق المعلوماتية لجامعة محمد الشريف مساعديّة سوق أهراس وأتعهد بالالتزام به.

التاريخ : التوقيع