



ميثاق تكنولوجيا المعلومات لجامعة سطيف 1- فرحات عباس

النسخة 1.0

الإصدار 2024

Setif 1 University - Ferhat ABBAS

هذا الميثاق الخاص بتكنولوجيا المعلومات قابل للمراجعة والتعديل والتحديث، بما يتماشى مع التطورات التكنولوجية والنصوص التنظيمية السارية المفعول.

تعتمد جامعة سطيف 1- فرحات عباس نظاما للمعلومات والاتصال ضروريا لحسن سير الأنشطة الأكاديمية، والبيداغوجية، والعلمية، والمهنية.

ويشمل على وجه الخصوص شبكة معلوماتية وهاتفية وبرمجيات ومواقع ويب ومنصات إلكترونية ورسائل إلكترونية بالإضافة إلى تجهيزات معلوماتية ثابتة ومتنقلة.

يجب أن يقتصر نظام المعلومات والاتصالات وموارد تكنولوجيا المعلومات حصريا على الأغراض الأكاديمية والمهنية باستثناء الحالات التي تسمح بها المصالح المعنية.

كما يمكن لأطراف ثالثة الوصول إلى التجهيزات المعلوماتية وأنظمة المعلومات والاتصالات التابعة للجامعة.

يهدف هذا الميثاق المعلوماتي إلى تحديد القواعد والحقوق المتعلقة باستخدام جميع الوسائل المعلوماتية المتاحة على مستوى هياكل جامعة سطيف 1- فرحات عباس وتوضيح مسؤوليات المستخدمين (أساتذة وطلبة وموظفي الإدارة والتقنيين والخدمات).

مما يتيح استخداما مناسباً وأمثلاً لموارد تكنولوجيا المعلومات المتوفرة، مع ضمان حد أدنى من مستوى الأمان الملائم للوسط الجامعي. كما يسعى إلى توعية المستخدمين بالمخاطر المرتبطة بسلامة وسرية المعلومات المعالجة والموارد المستخدمة.

يعمم الميثاق على جميع المستخدمين ويتم إعلامهم تلقائياً بكل تحديث أو تعديل يطرأ عليه. وفي هذا الإطار، يتم تذكير جميع المستخدمين بمضمونه بصفة دورية، ويكون الميثاق متاحاً للاطلاع عليه عبر الموقع الرسمي للجامعة.

وتنظم بشكل دوري أنشطة داخلية للتواصل والإعلام والتوعية، بهدف الحفاظ على مستوى كاف من المعلومات حول الممارسات السليمة الموصى بها.

1 الأهداف

يهدف هذا الميثاق إلى:

1.1 توعية المستخدمين بالمخاطر المرتبطة بأمن تكنولوجيا المعلومات فيما يتعلق بالحريات والخصوصية ولاسيما من خلال عمليات معالجة البيانات ذات الطابع الشخصي.

2.1 إعلام المستخدمين بمايلي:

-الاستخدامات المسموح بها للوسائل وموارد تكنولوجيا المعلومات الموضوعة تحت تصرفهم .

- قواعد الأمن المعمول بها.

- إجراءات الرقابة التي تتخذها جامعة فرحات عباس.

- العقوبات التي قد يتعرض لها المستخدمون عند الاقتضاء.

3.1 وضع القواعد العامة المتعلقة بأمن تكنولوجيا المعلومات وإضفاء الطابع الرسمي عليها، والتي يلتزم المستخدمون باحترامها مقابل إتاحة أنظمة المعلومات والتجهيزات والوسائل المعلوماتية لهم، بما يضمن تحديد حقوقهم وواجباتهم.

2. تعريف المفاهيم

1.2 موارد تكنولوجيا المعلومات

تشمل كل الوسائل المادية والبرمجيات بالإضافة إلى إمكانية الوصول إلى شبكة الويب، الشبكة الداخلية والبريد الإلكتروني المتاحة داخل الجامعة أو التي يمكن الوصول إليها من خارج الحرم الجامعي.

نذكر منها على وجه الخصوص الشبكات والخوادم، ومحطات العمل والبرمجيات والتطبيقات والمواقع والمنصات الإلكترونية، كذلك قواعد البيانات وأجهزة التوجيه والمبدلات الشبكية ونقاط الوصول إلى شبكة الواي فاي (Wi-Fi)، والكابلات والطابعات وأجهزة المسح الضوئي والهواتف المعتمدة على بروتوكول الإنترنت، والأقراص، وأقراص التخزين وغيرها.

2.2 ملكية موارد تكنولوجيا المعلومات

تعود ملكية جميع موارد تكنولوجيا المعلومات الموضوعة تحت تصرف المستخدمين حصريا إلى جامعة سطيف1- فرحات عباس. كما تعد جميع البيانات المخزنة على أجهزة الجامعة أو التي تمر عبر شبكاتها ملكا حصريا لها.

3.2 المستخدمون المعنيون

تسري قواعد وصلاحيات الولوج على جميع المستخدمين الذين لديهم ولوج دائم أو مؤقت إلى موارد الجامعة ومن بينهم: الأساتذة والطلبة وطلبة الدكتوراه، والباحثون والموظفون والأعوان الإداريون والتقنيون، والأساتذة المتعاقدون والمؤقتون والمتربصون والضيوف وغيرهم من المستخدمين.

4.2 خدمات الإنترنت

توفير مجموعة من الخدمات ووسائل تبادل المعلومات والاتصال، من خلال الخوادم المحلية أو مختلف وسائل الاتصال ولاسيما خدمات الويب والبريد الإلكتروني والمننديات، والاتصالات الهاتفية عبر بروتوكول الإنترنت (IP) والاجتماعات المرئية.

3 نطاق التطبيق

تنطبق القواعد المنصوص عليها في هذا الميثاق على جميع الموارد المعلوماتية التي توفرها الجامعة. كما تشمل جميع المستخدمين المستفيدين من هذه الموارد، وذلك على مستوى أحرار وهياكل جامعة سطيف1- فرحات عباس، سواء داخل الحرم الجامعي أو خارجه.

4 صلاحيات الولوج إلى موارد تكنولوجيا المعلومات

1.4 تمنح صلاحيات الولوج إلى الموارد المعلوماتية لكل مستخدم في الحدود المخولة له، وتعد هذه الصلاحيات شخصية، وغير قابلة للتنازل أو الاتاحة للغير سواء بصفة دائمة أو مؤقتة.

2.4 يجوز للجامعة تقييد صلاحيات الولوج أو سحبها بصفة تحفظية، في حالة عدم توافق سلوك المستخدم مع أحكام هذا الميثاق.

3.4 يحظر على المستخدم بأي شكل من الأشكال أن يسمح لشخص آخر الولوج إلى موارد الجامعة عن طريق استخدام بيانات اعتماده الخاصة وفي هذه الحالة، يتحمل المستخدم مسؤولية جميع الإجراءات التي يتم تنفيذها باستخدام معرفاته.

4.4 يجب إبلاغ الجامعة فوراً في حالة فقدان أو سرقة أو إفشاء معلومات المصادقة.

5 شروط الاستخدام

1.5 لا يجوز استخدام موارد تكنولوجيا المعلومات الموضوعة تحت تصرف الجامعة إلا لأغراض مهنية.

2.5 يقتصر الولوج إلى أي مورد معلوماتي على الأشخاص المصرح لهم بذلك رسمياً والمعرفين من قبل الجامعة. ويجوز بالنسبة لبعض التطبيقات الخاصة طلب الحصول على ترخيص مسبق من الجهة المسؤولة عن المورد المعني.

3.5 يمنح حق الولوج حصرياً في إطار الأنشطة والمهام المسموح بها داخل المؤسسة، ولا يجوز استعماله لأي غرض أو نشاط آخر خارج الإطار المحدد.

6 مسؤوليات الجامعة

1.6 توفير موارد تكنولوجيا المعلومات اللازمة للمستخدمين، بما يتناسب مع المهام والمسؤوليات الموكلة لهم.

2.6 ضمان حسن سير موارد تكنولوجيا المعلومات وتوفيرها .

3.6 العمل على ضمان جودة الخدمات المقدمة للمستخدمين في حدود الإمكانيات والموارد المخصصة.

4.6 إعلام المستخدمين بالإجراءات والسياسة المعمول بها والمتعلقة بموارد تكنولوجيا المعلومات.

5.6 توفير الوسائل اللازمة لضمان سرية وسلامة وثائق المستخدمين ومبادلاتهم الإلكترونية.

6.6 إعلام المستخدمين بأن الأنشطة التي يتم تنفيذها عبر الشبكة والأنظمة المعلوماتية تخضع للمراقبة الآلية.

7.6 توعية المستخدمين بالمخاطر المرتبطة بأمن المعلومات.

7 مسؤوليات المستخدم

1.7 الالتزام باحترام جميع القوانين واللوائح المعمول بها داخل الجامعة.

2.7 الالتزام بأحكام هذا الميثاق، وبمختلف الإجراءات والسياسات والقواعد المعتمدة من طرف الجامعة.

3.7 التطبيق الصارم لتدابير وتعليمات أمن المعلومات المعتمدة من طرف الجامعة.

4.7 يحظر استخدام أو محاولة استخدام حسابات المستخدمين الآخرين.

5.7 يتحمل المستخدم المسؤولية الكاملة لكل استخدام لوسائل المصادقة التي تضعها الجامعة تحت تصرفه.

6.7 يلتزم المستخدم، في حالة الغياب ولو لفترة وجيزة، بقل الوصول إلى المعدات الموضوعه تحت تصرفه.

7.7 يلتزم المستخدم بعدم تثبيت أو نسخ البرامج والملفات التي من شأنها أن تعرض أمن موارد الجامعة المعلوماتية للخطر.

8.7 يحرص المستخدم على احترام سرية المعلومات التي بحوزته، كما يلتزم في جميع الظروف، باحترام التشريعات والتنظيمات المعمول بها، ولا سيما تلك المتعلقة بحماية حقوق الملكية الفكرية، وسرية المراسلات والبيانات الشخصية، وأنظمة المعالجة الآلية للبيانات.

8 أخلاقيات استخدام تكنولوجيا المعلومات

يلتزم كل مستخدم باحترام قواعد وأحكام أخلاقيات استخدام تكنولوجيا المعلومات، والامتناع عن القيام عمدا بأي أعمال أو عمليات قد من شأنها أن تؤدي إلى ما يلي:

1.8 إخفاء هويته الحقيقية.

2.8 المساس بصورة الجامعة أو بسمعتها أو بنزاهتها.

3.8 تغيير أو تعديل البيانات، أو الوصول إلى المعلومات الخاصة بمستخدمين آخرين أو بالجامعة دون الحصول على التصريح أو الموافقة اللازمة.

4.8 تعطيل وعرقلة السير العادي للشبكة أو لأي نظام من الأنظمة المتصلة بها.

5.8 تعديل أو إتلاف المعلومات الموجودة على أحد الأنظمة.

6.8 الدخول أو محاولة الدخول إلى موقع أو نظام دون الحصول على تصريح بذلك.

7.8 محاولة اعتراض الاتصالات المتبادلة بين أطراف أخرى.

9 حماية محطة العمل

1.9 قفل الدخول إلى محطة العمل في حالة الغياب، حتى لو كان بصفة مؤقتة.

2.9 إبلاغ المصالح التقنية في حال فتح أي جهاز جديد بمحطة العمل.

3.9 التأكد من أن محطة العمل مزودة ببرنامج مضاد للفيروسات، وإبلاغ المصلحة المعنية بأي تنبيه أمني.

4.9 يمنع منعاً باتاً توصيل أي أجهزة شخصية بمحطة العمل.

5.9 فحص جميع وسائط التخزين القابلة للإزالة المتصلة بمحطة العمل قبل استخدامها.

6.9 إيقاف تشغيل الحاسوب خلال فترات عدم الاستخدام الطويلة (ليلاً، عطلة نهاية الأسبوع، العطل إلخ).

7.9 عدم إجراء أي تدخل مادي أو تقني على المعدات.

10 البريد الإلكتروني

- 1.10** يلتزم المستخدم بعدم مشاركة بيانات الدخول إلى حساب البريد الإلكتروني الممنوح له من طرف الجامعة مع أي شخص آخر.
- 2.10** يلتزم المستخدم باستخدام كلمة مرور قوية تتكون من أحرف وأرقام، وتتضمن رموزاً خاصة وأحرف كبيرة، مع تغييرها بصفة دورية.
- 3.10** لا يجوز استخدام البريد الإلكتروني في المواقع التي قد تشكل أخطار أمنية على حساب المستخدم أو على موارد الجامعة.
- 4.10** يجب على كل مستخدم إنشاء توقيع خاص به، يتضمن معلومات الاتصال الخاصة به، واستخدامه في كل رسالة يتم إرسالها.
- 5.10** عدم فتح الملفات أو الروابط المرسلة من عناوين بريد إلكتروني مجهولة وغير معروفة.
- 6.10** يجب على كل مستخدم تنظيم واتخاذ الوسائل لحفظ الرسائل الإلكترونية التي قد تكون ضرورية.
- 7.10** تقع مسؤولية استخدام وإدارة حساب البريد الإلكتروني على عاتق المستخدم.
- 8.10** يمنع استخدام البريد الإلكتروني لأغراض شخصية أو حزبية.
- 9.10** تخضع الرسائل الإلكترونية المستلمة عبر البريد الإلكتروني المهني للفحص ضد الفيروسات ولتصفية الرسائل غير المرغوب فيها (Spam). ويطلب من المستخدمين إبلاغ مركز الأنظمة والشبكات عن أي أعطال يلاحظونها في نظام التصفية.
- 10.10** يخضع إرسال الرسائل الإلكترونية إلى أطراف أخرى، للقواعد نفسها المطبقة على علو إرسال المراسلات البريدية، ولا سيما فيما يتعلق بالتنظيم الهرمي. وفي حالة الشك بشأن الجهة أو الشخص المخول بإرسال الرسالة، يجب الرجوع إلى مركز الأنظمة والشبكات.
- 11.10** يجب أخذ بعين الاعتبار أخطار التأخر وعدم تسليم الرسائل والحذف التلقائي للرسائل الإلكترونية عند إرسال المراسلات المهمة. ويرسل البريد الإلكتروني المهم مع طلب إشعار بالاستلام أو يكون موقعاً إلكترونياً.

12.10 يسمح بإرسال الرسائل الإلكترونية إلى عدد محدد من المستلمين، وفقا للعدد الذي يحدده مركز الأنظمة والشبكات وذلك لأسباب تقنية، مع إمكانية رفع هذا الحد مؤقتا بناءا على طلب المستخدمين.

13.10 وبالمثل، يمكن لمركز الأنظمة والشبكات تحديد حجم ونوع وعدد الملفات المرفقة، وذلك لتجنب حدوث ضغط أو ازدحام في نظام البريد الإلكتروني.

11 الإنترنت والشبكة الداخلية والاتصال

1.11 يتاح الوصول إلى شبكة الويب عبر البنية التحتية للجامعة لأغراض التعليم، والبحث العلمي والتسيير والإدارة.

2.11 يحظر استخدام هذه الخدمة لأغراض ضارة، أو إباحية، أو احتيالية، أو تحريرية على الكراهية أو غير قانونية.

3.11 يجب تحميل الملفات، ولا سيما الملفات الصوتية والصور ومقاطع الفيديو من شبكة الويب بما يحترم حقوق الملكية الفكرية، وألا يتجاوز نطاق الأنشطة الأكاديمية والتعليمية، والبحث العلمي والتسيير والإدارة.

4.11 يمنع منعاً باتاً تحميل ملفات الفيديو أو الصوت أو البرامج ذات الحجم الكبير، والتي قد تتسبب في إبطاء الوصول على شبكة الويب بالنسبة لبقية المستخدمين.

5.11 يجب أن تخضع أي عملية نشر لصفحات معلومات أو وثائق على الموقع الرسمي للجامعة أو شبكتها الداخلية، لموافقة مسؤول الموقع أو مسؤول النشر المعين رسمياً لهذا الغرض.

6.11 يمنع منعاً باتاً استخدام الشبكة، أو أي حاسوب أو خادم أو مودم أو جهاز توجيه أو تجهيز آخر لتوفير خدمة يمكن الوصول إليها عبر شبكة الويب، مثل خدمة بروتوكول سطح المكتب البعيد RDP.

7.11 يمنع على المستخدم انتحال شخصية أو هوية الآخر، كما يحظر عليه اعتراض الاتصالات المتبادلة بين أطراف أخرى.

8.11 لا يجوز للمستخدم تخزين أو إيداع بيانات على خادم داخلي أو على خوادم مفتوحة لعامة المستخدمين مثل (Google و Free و Orange وغيرها) ، أو على محطة عمل مستخدم آخر إلا بعد الحصول على تصريح المسؤولين المخولين بذلك.

9.11 يسمح باستخدام الإنترنت لأغراض شخصية في حدود معقولة، شرط ألا تؤدي عملية التصفح إلى عرقلة أو التأثير سلباً على الوصول إلى الخدمات والموارد اللازمة للأغراض المهنية.

10.11 يخضع إدراج نقاط الوصول (Access Points) ، وأجهزة المودم (Modem) ، والمبدلات الشبكية (Switch) ضمن الشبكة إلى الموافقة المسبقة من مهندس الشبكة.

12 الأجهزة المحمولة ووسائط التخزين

يجب على المستخدم :

1.12 إبلاغ المسؤولين المباشرين فوراً عن أي فقدان أو سرقة لجهاز محمول أو وسيط تخزين مهني.

2.12 الحرص دائماً على قفل الأجهزة المحمولة عندما لا تكون قيد الاستعمال.

3.12 تعطيل وظائف الواي فاي والبلوتوث في الأجهزة عندما لا تكون هناك حاجة إليها

4.12 يُمنع منعاً باتاً على أي شخص من خارج الجامعة نقل الوثائق باستخدام وسائط التخزين القابلة للإزالة؛ ويجب أن تتم جميع عمليات تبادل الوثائق عبر البريد الإلكتروني. وفي حالة الحاجة إلى نقل حجم كبير من البيانات يستوجب استخدام وسيط تخزين قابل للإزالة، يجب إخضاع هذا الوسيط للفحص من طرف المصالح المختصة قبل استعماله.

5.12 تشفير البيانات السرية الموجودة على الأجهزة المحمولة ووسائط التخزين.

6.12 أثناء التنقلات المهنية، يجب على المستخدمين الاحتفاظ بالأجهزة المحمولة ووسائط التخزين القابلة للإزالة، بحوزته الشخصية.

13 وسائل التواصل الاجتماعي

1.13 يجب أن تتم إدارة الحسابات الرسمية من طرف أشخاص تعينهم الجامعة.

2.13 يجب أن تكون كل المنشورات متوافقة مع قيم الجامعة وصورتها وسمعتها.

3.13 يجب أن يقتصر استخدام شبكات التواصل الاجتماعي أثناء ساعات العمل على الاستخدام المهني.

4.13 تمنع مشاركة أي معلومات سرية تتعلق بالجامعة أو أعضائها أو أنشطتها دون الحصول على ترخيص مسبق.

5.13 يجب أن تعكس الآراء المنشورة عبر الإنترنت وجهات نظر أصحابها، وألا تلزم الجامعة أو ترتب عليها أي مسؤولية إلا في حال وجود تصريح مباشر بذلك.

6.13 يجب احترام حقوق المؤلف والملكية الفكرية عند مشاركة المحتويات.

7.13 يجب الإبلاغ عن أي سلوك غير لائق إلى الجهات المختصة في الجامعة.

14 تدابير الأمن الواجب تطبيقها أثناء التنقلات إلى الخارج

1.14 يمنع استخدام أجهزة طرفية عامة أو مشتركة للوصول إلى حساب البريد الإلكتروني المهني أو التطبيقات المهنية.

2.14 يتعين على الموظف تعطيل وظائف الاتصال اللاسلكي مثل الواي فاي والبلوتوث في أجهزته عندما لا تكون هناك حاجة إليها.

3.14 يجب على الموظف الاحتفاظ بجهازه المهني ووسائط التخزين الخاصة به بحوزته بشكل دائم.

4.14 يجب على الموظف حذف جميع البيانات المهنية الحساسة وغير الضرورية للمهمة من جميع وسائط التخزين القابلة للإزالة قبل أي تنقل للخارج.

5.14 يجب على الموظف إبلاغ المسؤولين والتمثيلية الدبلوماسية الجزائرية في حالة تفتيش أو حجز معدات الإعلام الآلي من طرف السلطات الأجنبية أثناء المهام في الخارج.

6.14 يمنع استخدام المعدات المقدمة أو الممنوحة أثناء التنقل للخارج لأغراض شخصية.

7.14 يجب على الموظف إدراج قائمة بالأجهزة المتصلة والممنوحة أثناء التنقل ضمن التقرير الخاص بالمهمة.

8.14 يمنع منعاً باتاً على أي شخص أجنبي نقل الوثائق باستخدام وسائط التخزين القابلة للإزالة، حصرياً عبر البريد الإلكتروني.

9.14 يجب على الموظف تغيير كلمات المرور التي استخدمها أثناء المهمة.

15 الأمن

يجب على المستخدمين الحرص على الالتزام الصارم بالقواعد واللوائح والتعليمات المعمول بها في أمن المعلومات، ويتعين عليهم، على وجه الخصوص قفل أجهزة العمل عند المغادرة،

ولاسيما في حالة الغياب لفترات طويلة، والامتناع عن توصيل أجهزة شخصية، والتأكد من توفر أدوات الفحص وبرامج مكافحة الفيروسات لجميع وسائط التخزين القابلة للإزالة.

كما يتعين على المستخدمين الالتزام بالتعليمات التالية:

1.15 الحرص على عدم إدخال ملفات ذات حجم كبير إلى شبكات المعلومات.

2.15 الحرص على عدم إدخال فيروسات إلى الشبكات سواء كانت قادمة من أقراص التخزين المحمولة أو من مواقع الويب الخطيرة، أو من حساب البريد الإلكتروني الخاص بالمستخدم.

3.15 التحقق جيدا من مواقع الويب التي يتم الدخول إليها، وتجنب المواقع الخطيرة.

تحتفظ جامعة سطيف1- فرحات عباس بحقها في تصفية أو حظر الولوج إلى بعض المواقع، وإجراء مراقبة مسبقة أو لاحقة للمواقع التي تمت زيارتها، وكذلك للمدة الزمنية التي تم قضاؤها في الولوج إليها.

ملاحظة: تم إعداد دليل للممارسات الجيدة المتعلقة بأمن تكنولوجيا المعلومات في جامعة سطيف1- فرحات عباس، ويتعين على جميع مستخدمي موارد تكنولوجيا المعلومات الالتزام به.

16 الإطار القانوني

يلتزم مستخدمو موارد تكنولوجيا المعلومات باحترام القوانين المتعلقة بالملكية الأدبية والفنية، وكذلك القوانين المرتبطة بها فيما يخص المسؤولية المدنية والجنائية والمهنية، ويشمل ذلك على وجه الخصوص احترام الالتزامات التالية:

1.16 احترام حقوق المؤلف (الحقوق المعنوية والمالية وحقوق النشر والتوزيع).

2.16 احترام الحياة الخاصة للغير، حيث يمنع نشر صورهم أو معلوماتهم دون احترام حقهم في الخصوصية.

3.16 يمنع انتحال الهوية والسرقة والتشهير ونشر المعلومات الشخصية أو السرية، أو المعلومات التي تشكل انتهاكا للسلامة الجسدية أو المعنوية للشخص.

4.16 احترام التزامات قانون "المعلومات والحريات" (القانون رقم 03-07، والأمر رقم 03-05 المؤرخ في 19 يوليو 2003، المتعلق بحقوق المؤلف والحقوق المجاورة.

والقانون رقم 07-18 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي).

17 السرية

1.17 تكون بيانات المستخدم خاصة وسرية باستثناء حالات الخطر أو الأحداث الخاصة.
2.17 يلتزم كل مستخدم مسموح له بالولوج إلى بيانات وموارد خاصة بالجامعة، بالحفاظ على سرية المعلومات التي يصل إليها في إدارة مهامه.

3.17 يتم حماية الولوج إلى بعض عناصر نظام المعلومات مثل البريد الإلكتروني أو الهاتف والأجهزة والجلسات على أجهزة العمل والشبكة وبعض التطبيقات والخدمات التفاعلية، بواسطة بيانات تسجيل الدخول، مثل اسم المستخدم وكلمة المرور.

4.17 يجب على المستخدم أن يحفظ بيانات تسجيل الدخول في ذاكرته قدر الإمكان، والاحتفاظ بها أو تخزينها بأي شكل من الأشكال، وفي جميع الأحوال، يمنع إفشاؤها أو نقلها إلى أشخاص آخرين أو جعلها سهلة الوصول إليها. ويجب على المستخدم إدخالها في كل مرة يريد فيها الدخول وألا يتم حفظها تلقائياً في ذاكرة نظام المعلومات.

18 إدارة الحوادث الأمنية

في حالة وقوع حادث يمكن أن يؤثر على أمن تكنولوجيا المعلومات، يجوز للجامعة اتخاذ الإجراءات التالية:

1.18 قطع اتصال المستخدم مع أو دون إشعار مسبق، حسب خطورة الوضع.
2.18 عزل أو تعطيل أي بيانات أو ملفات بشكل مؤقت إذا كانت مخالفة لأحكام هذا الميثاق أو من شأنها أن تعرض أمن أنظمة المعلومات للخطر.
3.18 إبلاغ المسؤول الإداري المباشر.

19 العقوبات المطبقة

1.19 يحمل المستخدم مسؤولية عدم احترام القواعد المنصوص عليها في هذا الميثاق، وقد يؤدي ذلك إلى اتخاذ تدابير تأديبية بحقه، تكون متناسبة مع خطورة الأفعال المثبتة.
2.19 شرط إبلاغ المسؤول المباشر، يجوز للمسؤولين عن أمن تكنولوجيا المعلومات تنبيه المستخدم أو تقييد أو سحب صلاحيات ولوجه مؤقتاً، كما يجوز لهم حذف، أو ضغط، أو

عزل أي بيانات أو ملفات مخالفة لأحكام الميثاق أو من شأنها أن تعرض أمن أنظمة المعلومات للخطر.

3.19 تحال حالات الغش، وعدم احترام القواعد والإخلال بحسن سير المؤسسة إلى اللجنة التأديبية لجامعة فرحات عباس سطيف 1، التي تتولى إصدار العقوبات.

20 انتهاء العلاقة بين المستخدم وجامعة سطيف 1- فرحات عباس

1.20 عند انتهاء العلاقة التي تربط المستخدم بالجامعة، يتعين على المستخدم إعادة جميع موارد تكنولوجيا المعلومات المادية التي وضعت تحت تصرفه إلى المؤسسة.

2.20 تقوم المؤسسة بحذف جميع موارد تكنولوجيا المعلومات التي وضعتها تحت تصرف المستخدم.

21 دخول الميثاق حيز التنفيذ

يدخل هذا الميثاق حيز التنفيذ فوز اعتماده من طرف الهيئات التداولية الجامعية، والمتمثلة

- المجلس العلمي

- مجلس الإدارة

وسيتم نشره بالوسائل القانونية المعتمدة في الجامعة، كما سيتم إدراجه ضمن النظام الداخلي لجامعة فرحات عباس سطيف 1.

22 الالتزام الفردي

يتعين على جميع أفراد الأسرة الجامعية، من أساتذة وطلبة وموظفين والتزامهم باحترام جميع الأحكام المنصوص عليها في هذا الميثاق.

كما يتعين عليهم ملء خانات المعلومات الواردة في الإطار أدناه وكتابة عبارة "اطلعت ووافقت" ثم التوقيع على الوثيقة.

أنا الممضي أسفله،

الاسم واللقب:

الوظيفة/ الرتبة:

الكلية/ المصلحة:

القسم:

المستخدم لموارد الاعلام الآلي وشبكات جامعة سطيف 1- فرحات عباس.
أشهد وأقر بأنني اطلعت على هذا الميثاق، وألتزم باحترامه والتقيد بأحكامه.

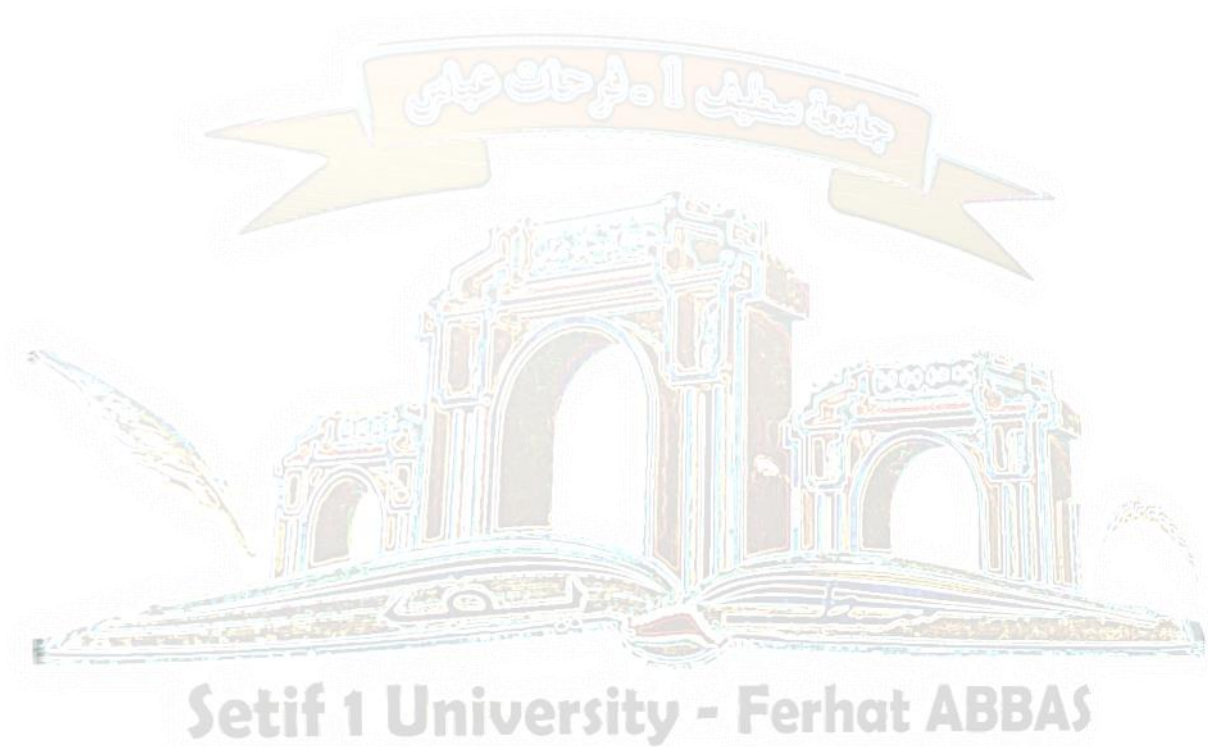
التاريخ والإمضاء:

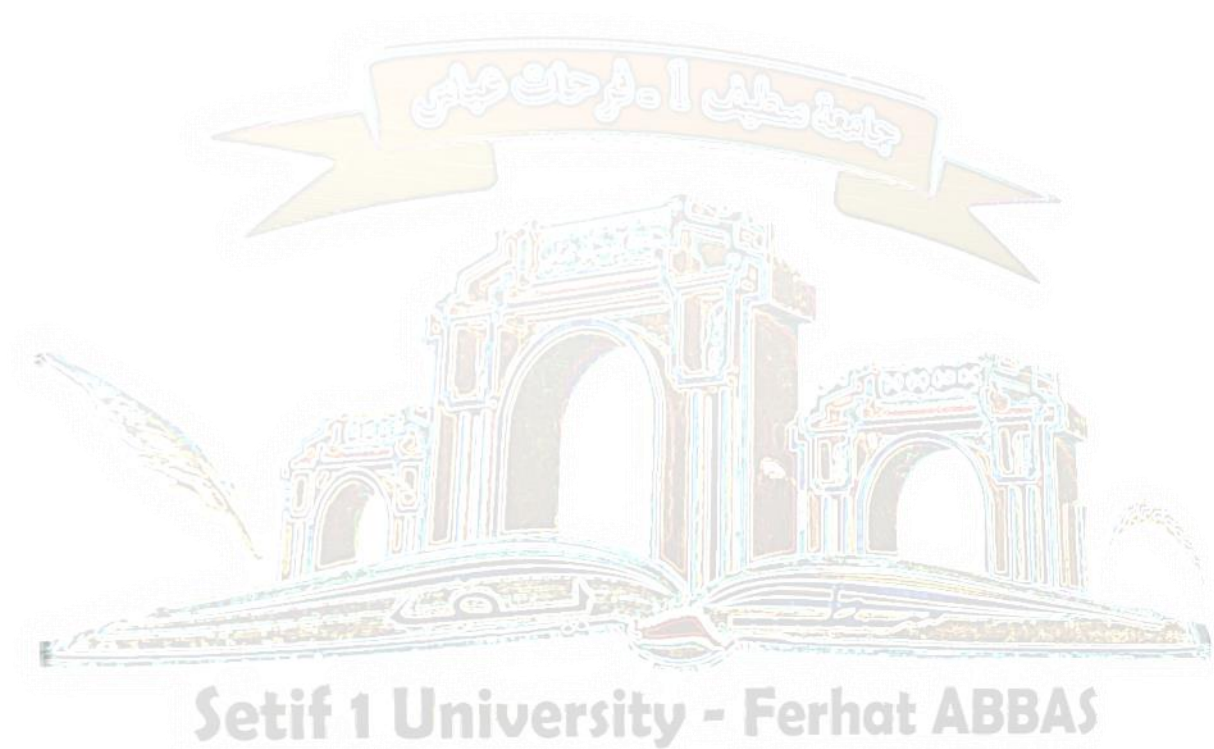


النصوص المرجعية

<u>المراجع</u>	<u>النص القانوني أو التنظيمي</u>
المرسوم التنفيذي رقم 61-16 المؤرخ في 02 جمادى الأولى 1437 الموافق لـ 11 فبراير 2016، المعدل والمتمم للمرسوم التنفيذي رقم 410-09 المؤرخ في 23 ذي الحجة 1430 الموافق لـ 10 ديسمبر 2009. المحدد لقواعد الأمن المطبقة على الأنشطة المتعلقة بالتجهيزات الحساسة.	<u>التنظيم المتعلق بالتدابير التشفيرية</u>
القانون رقم 04-18 المؤرخ في 24 شعبان 1439 الموافق لـ 10 مايو 2018، المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية.	<u>القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية</u>
الأمر رقم 05-03 المؤرخ في 19 جمادى الأولى 1424 الموافق لـ 19 يوليو 2003، المتعلق بحقوق المؤلف والحقوق المجاورة.	<u>الملكية الفكرية (البرمجيات)</u>
القانون رقم 04-15 المؤرخ في 11 ربيع الثاني 1436 الموافق لـ 01 فبراير 2015، المحدد للقواعد العامة المتعلقة بالتوقيع والمصادقة الإلكترونية. المرسوم رقم 134-2016 المؤرخ في 17 رجب 1437 الموافق لـ 25 أبريل 2016، المحدد لطبيعة وتشكيلة وتنظيم وسير السلطة الحكومية للمصادقة الإلكترونية. المرسوم رقم 135-2016 المؤرخ في 17 رجب 1437 الموافق لـ 25 أبريل 2016، المحدد لطبيعة وتشكيلة وتنظيم وسير السلطة الحكومية للمصادقة الإلكترونية.	<u>المصادقة الإلكترونية</u>
القانون رقم 07-18 المؤرخ في 25 رمضان 1439 الموافق لـ 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة البيانات ذات الطابع الشخصي.	<u>حماية المعطيات ذات الطابع الشخصي</u>
القانون رقم 04-09 المؤرخ في 14 شعبان 1430 الموافق لـ 05 أغسطس 2009، المتضمن	<u>المخالفات المرتبطة بتكنولوجيا الإعلام والاتصال</u>

القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها.	
المرسوم الرئاسي 14-252 المؤرخ في 13 ذي القعدة 1435 الموافق لـ 08 سبتمبر 2014، المتضمن المصادقة على الاتفاقية العربية لمكافحة الجرائم الإلكترونية.	<u>مكافحة الجرائم الإلكترونية</u>







Information Technology Charter Of Sétif 1 University- Ferhat Abbas

Version 0.1

2024 Edition

Setif 1 University - Ferhat ABBAS

This Information Technology charter may be modified and adjusted in accordance with technological development and applicable regulations.

Sétif 1 University- Ferhat Abbas implements an information and communication system necessary for the smooth running of academic, educational, scientific, and professional activities, including in particular, a computer and telephone network, software, websites and web platforms, email services as well as fixed and mobile equipment. Information and Communication system and IT resources shall be used exclusively for academic and professional purposes, except where specifically authorized by the relevant services. Furthermore, third parties may also have access to UFAS1's IT equipment and information and communication systems.

The IT charter aims to define the rules and rights governing the use of all IT resources available within the structures of the Sétif 1- University Ferhat Abbas, and to specify the responsibilities of users (faculty members, students and ATS) in order to ensure appropriate and optimal use of the available IT resources, while guaranteeing a minimum level of security suited to the academic environment. Likewise, this charter seeks to raise users' awareness of the risks related to the integrity and confidentiality of information processed and resources used.

The charter is disseminated to all users, who are systematically informed of each update made to it. As such, it is communicated to all users and available on the university's institutional website. Internal communication, information and awareness-raising are regularly organized to maintain a sufficient level of information regarding recommended good practices.

1. Objectives

This charter aims to:

1.1 Raise users' awareness of information security risks related to privacy and individual rights, particularly in connection with the processing of personal data they may be required to carry out.

1.2 Inform users about the authorized uses of the IT resources made available to them, the applicable information security rules, the monitoring and control measures implemented by UFAS1, and the sanctions to which users may be subject.

1.3 Formalize the general security rules that users undertake to comply with in return for access to information systems and IT equipment, thereby defining users' rights and obligations.

2. Definition of Terms

2.1 Information Technology Resources

IT resources include all hardware and software resources, as well as access to the web, the intranet, and email services, available within the university or accessible from outside the

campus. These resources encompass networks, servers, workstations, applications, websites and web platforms, databases, routers, switches, Wi-Fi access points, cables, printers and scanners, IP phones, hard drives, USB flash drives.

2.2 Ownership of Information Technology Resources

All IT resources provided to users are the exclusive property of the Sétif 1 University- Ferhat Abbas. Likewise, all data stored on the university's equipment or transmitted through its networks are the exclusive property of the university.

2.3 Applicable Users

The access rules and rights apply to all users with permanent or temporary access to the university's resources, including faculty members, students, doctoral candidates, researchers, employees, administrative and technical staff, part-time lecturers, interns, guests, etc.

2.4 Internet Services

Internet services consist of providing local servers or various means of information and communication, such as web services, email, forums, IP telephony, Videoconferencing...

3. Scope of Application

The rules set out in this charter apply to all IT resources provided by the university and to all users of these resources across all UFAS campuses and organizational units, both inside and outside the university campus.

4 Access Rights to Information Technology Resources

4.1 Access is granted to each user only within the limits of the privileges assigned to them. This right is personal and may not be transferred to any third party even temporarily. Access is established through the creation of **personal and confidential credentials for each user of the IT resources made available to them.**

4.2 Access rights may be limited or revoked as a precautionary measure, if the user's conduct does not comply with this charter.

4.3 Under no circumstances may a user allow another person to access the university's resources using their credentials. In such cases, the user shall be responsible for all actions performed using their credentials.

4.4 Any loss, theft, or disclosure of authentication information must be reported to the university immediately.

5. Terms of Use

5.1 The university's IT resources may be used only for professional purposes.

5.2 Access to IT resources is permitted only to duly authorized and identified university users. Prior authorization from the entity responsible for the relevant resource may be required for specific applications.

5.3 Access rights are limited to activities that comply with the requirements of the relevant entity and may not be used for any other activities outside the defined scope.

6. University Responsibilities

6.1 Provide users with IT resources required to carry out their duties.

6.2 Ensure the proper functioning and availability of IT resources.

6.3 Maintain the quality of services provided to users within the limits of the resources allocated.

6.4 Inform users of the applicable procedures and policies relating to IT resources.

6.5 Implement the necessary measures to ensure the confidentiality and integrity of users' documents and electronic communications.

6.6 Inform users that activities carried out on the network and information systems are subject to automated monitoring.

6.7 Raise users' awareness of information security risks.

7. User Responsibilities

7.1 Comply with applicable laws and regulations.

7.2 Comply with this charter, as well as the university's policies and procedures.

7.3 Strictly adhere to the university's IT security measures and guidelines.

7.4 Do not use or attempt to use another user's account.

7.5 The user is solely responsible for the use of authentication credentials provided to them by the university.

7.6 In the event of any absence, even temporary, the user must ensure that access to the equipment assigned to them, or to their own equipment containing professional information, is locked.

7.7 The user must perform regular backups of the files stored on the equipment provided to them

7.8 The user must refrain from installing software, copying, or installing files that may pose security risks within the university.

7.9 The user must ensure the confidentiality of the information in their possession. Under all circumstances, they must comply with applicable legislation, which protects in particular intellectual property rights, the confidentiality of correspondence, personal data, and automated data processing systems.

8. Information Technology Code of Ethics

Each user undertakes to comply with the rules of IT ethics and must not intentionally perform any actions that may result in.

8.1 Concealing their true identity.

8.2 Damaging the image, reputation, or integrity of the university.

8.3 Altering or modifying data or accessing information belonging to other network users or to the university without their consent.

8.4 Interrupting or disrupting the normal operation of the network or any of the systems connected to the network.

8.5 Modifying or destroying information stored on any system.

8.6 Connecting or attempting to connect to a website or system without proper authorization.

8.7 Attempting to intercept communication between third parties.

9. Workstation Protection

9.1 Lock the workstations, whenever the user is absent, even temporarily.

9.2 Notify the technical services if any new device is connected to the workstation.

9.3 Ensure that the workstation is protected by antivirus software and report any security alerts to the appropriate IT support team.

9.4 Never connect personal devices to the workstation.

9.5 Scan all removable media connected before using them.

9.6 Shut down the computer during extended periods of inactivity (e.g. overnight, on weekends, during holidays, or vacation).

9.7 Do not physically tamper with the workstation hardware.

10. Email

10.1 The user must not share their credentials with anyone else.

10.2 The user must use a strong password consisting of alphanumeric characters, special characters and uppercases letters and change it regularly.

10.3 Email address must not be used on websites that may pose security risks to the user's account or the university's resources.

10.4 Each user must create their own email signature containing their contact information and use it in every outgoing message.

10.5 The user must not open files or links received from unknown email addresses.

10.6 Each user must organize and implement the necessary measures to retain any messages that may be essential.

10.7 The use and management of the email account is the responsibility of the user.

10.8 The email service must not be used for personal or partisan purposes.

10.9 Emails received through the professional email system are subject to antivirus scanning and anti-spam filtering. Users are encouraged to report any malfunctions they identify in the filtering system to the Systems and Networks Center.

10.10 Sending emails to third parties is subject to the same rules as sending postal correspondence, particularly regarding the hierarchical organization. In case of doubt about the appropriate sender authorized to send the message, users should refer the matter to the Systems and Networks Center.

10.11 The risk of delays, non-delivery, and automatic deletion of electronic messages must be taken into consideration when sending important correspondence. Important messages should be sent with a delivery receipt or an electronic signature.

10.12 For technical reasons, emails can only be sent directly to a limited number of recipients, as determined by the Systems and Networks Center. This limit may be temporarily lifted upon request.

10.13 Similarly, the size, number, and type of attachments may be limited by the Systems and Networks Center to prevent the email system from being overloaded.

11. Internet, Intranet, Connectivity

11.1 Access to the web through the university infrastructure is available for educational, research and governance purposes.

11.2 This service must not be used for any malicious, obscene, fraudulent, hateful, defamatory, or illegal purposes.

11.3 Any downloading of files including audio, images or videos files from the Web must comply with intellectual property rights and must remain within the scope of academic, educational, research and governance activities.

11.4 Downloading of large video, audio or software files that may slow down web access for other users is strictly prohibited.

11.5 Any publication of information pages or documents on UFAS1 websites or intranet sites must be approved by a specifically designated website manager or publication manager.

11.6 The use of a network or any PC, server, modem, router or other equipment to provide a web accessible service, such as RDP (Remote Desktop Protocol) is strictly prohibited.

11.7 The user must not impersonate another person or intercept communications between third parties.

11.8 The user must not upload data to an internal server, a publicly accessible server (Google, Free, Orange, etc.), or another user's workstation without prior authorization from the authorized personal.

11.9 The use of the Internet for private purposes is tolerated within reasonable limits, provided that browsing does not interfere with professional access.

11.10 The installation of access points, modems, switches, or any other network equipment on the network requires prior authorization from the network engineer.

12. Mobile Devices and Storage Media

Users must:

12.1 Immediately report to their supervisor any loss or theft of a work-related mobile device or storage medium.

12.2 Always lock mobile devices when they are not in use.

12.3 Disable the Wi-Fi and Bluetooth functions of devices whenever they are not needed. **12.4** It is strictly prohibited for individuals who are not affiliated with the university to transfer documents using removable storage media. All document exchanges must be carried out by email. Where the volume of data requires the use of removable media, the device must be scanned by the appropriate university services before use.

12.5 Encrypt confidential data stored on mobile devices and storage media.

12.6 During business trips, users must keep their mobile devices and removable storage media in their possession at all times.

13. Social Media

13.1 Official social media accounts must be managed by individuals designated by the university.

13.2 All publications must comply with the university's values and uphold its image.

13.3 The use of social media during working hours must be limited to professional purposes.

13.4 The user must not share confidential information regarding the university, its members or its activities without prior authorization.

13.5 Opinions shared online must clearly be your own and must not imply or incur liability on the part of the university unless explicitly authorized.

13.6 Respect copyright and intellectual property rights when sharing content.

13.7 Report any inappropriate behavior to the appropriate authorities.

14. Security Measures to Follow When Travelling Abroad

14.1 The use public or shared devices to access professional email accounts or business applications, is prohibited

14.2 Employees travelling on official business must disable wireless communication features, such as Wi-Fi and Bluetooth, on their devices whenever they are not required.

14.3 Employees on official business must keep their work-issued device and any storage media with them at all times.

14.4 Before travelling abroad, the employees must remove all sensitive work-related data that is not required for the assignment from all removable storage media.

14.5 The employees must inform their supervisor and the Algerian diplomatic mission in the event that their information technology equipment is inspected or seized by foreign authorities during official travel abroad.

14.6 It is prohibited to use equipment received during travelling abroad for personal purposes.

14.7 The employees must include in the mission reports a list of connected devices received as gifts during the trip.

14.8 It is strictly prohibited for a foreign national to transfer documents using removable storage media. All document exchanges must be carried out exclusively via email.

14.9 The employees must change the passwords used during the mission.

15. Security

Users must comply with all applicable laws, regulations and information security guidelines. In particular, they must lock their workstation whenever they are away from it, especially during extended absences. They refrain from connecting personal devices and ensure that all removable media are scanned and protected by antivirus and software.

Users are required to comply with the following instructions:

15.1 Ensure that large files are not uploaded to the computer network.

15.2 Ensure that viruses are not introduced into the network through their USB flash drives, malicious websites, or their email accounts.

15.3 Users must check and verify the websites they access and avoid malicious websites.

UFAS1 reserves the right to filter or block access to certain websites and to monitor, either before or after the fact, the websites visited and the corresponding access durations

N.B. An information security best practice guide for UFAS1 has been established and must be followed by all users of UFAS's IT resources.

16. Legal Framework

Users of the university's IT resources must comply with laws relating to literary and artistic property, as well as the laws associated with civil, criminal, and professional liability. This particularly implies compliance with the following obligations, without this constituting an exhaustive list:

16.1 Comply with copyright law including moral rights, economic rights, and the right of dissemination.

16.2 Respect the privacy and image rights of others.

16.3 The prohibition of identity theft, theft, defamation and the dissemination of personal or confidential information or any information constituting a violation of an individual's physical or moral integrity.

16.4 **Complying** with the requirements of the “**Informatique et Libertés**” law, including

Law No. 03-17, Ordinance No. 03-05 of 19 July 2003 on the Protection of Copyright and Related Rights, and Law No. 18-07 of 10 June 2018 on the Protection of Natural Persons in the Processing of Personal Data.

17. Confidentiality

17.1 A user's data must be considered private if it is clearly identified as such, except in the event of a specific risk or circumstance. Access to a user's private data requires the user's consent.

17.2 Any user authorized to access the university's data and IT resources must maintain the confidentiality of any information to which they have access in the course of their duties.

17.3 Access to certain components of the information system (such as email or telephone services, workstation sessions, the network, and certain applications or interactive services) is protected by login credentials (usernames and passwords).

17.4 Whenever possible, these credentials must be memorized by the user and must not be stored in any form whatsoever. In any event, they must not be disclosed to third parties or made easily accessible. They must be entered by the user each time access is required and must not be stored in the information system's memory.

18. Incident Management

In the event of an incident that may affect security, the university may:

18.1 Disconnect a user, with or without prior notice depending on the severity of the situation.

18.2 Isolate or temporarily disable any data or file that is inconsistent with this charter or that could compromise the security of the information systems.

18.3 Notify the user's immediate supervisor.

19. Applicable Sanctions

19.1 Failure to comply with the rules set out in this charter may result in the user being held liable and may lead to disciplinary measures proportionate to the seriousness of the established facts.

19.2 Subject to informing the immediate supervisor, the IT security officers may issue a warning to a user, temporarily restrict or revoke the user's access rights and delete, compress or isolate any data or files that violate this charter or that may compromise the security of information systems.

19.3 Cases involving fraud, non-compliance with the rules, or actions that adversely affect the proper functioning of the institution shall be referred to the UFAS1 Disciplinary Committee, which shall impose the appropriate sanctions.

20. Termination of The relationship between the User and UFAS1

20.1 When the relationship between the user and the university comes to an end, the user must return all IT hardware resources made available to them.

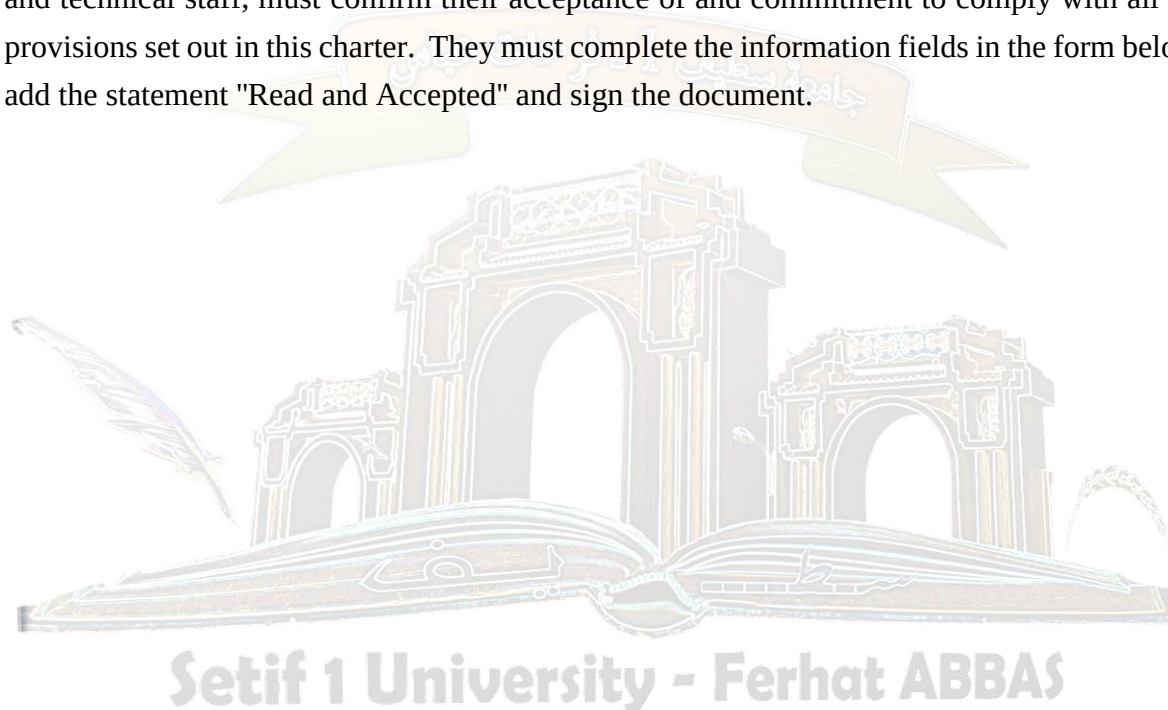
20.2 The institution shall delete all IT resources made available to the user.

21. Entry into Force of the Charter

This charter shall enter into force upon its adoption by the university's deliberative bodies, namely the Scientific Council and the Board of Directors. It shall be published through the university's official legal channels and shall be incorporated into UFAS1's internal regulations.

22. Individual Commitment

All members of the university community, including faculty members, students, administrative and technical staff, must confirm their acceptance of and commitment to comply with all the provisions set out in this charter. They must complete the information fields in the form below, add the statement "Read and Accepted" and sign the document.



I, the undersigned

Full name:

Profession/Grade:

Faculty/Service:

Department:

As a user of IT resources and networks of Sétif 1 University- Ferhat Abbas, I certify and affirm that I have read this charter and undertake to abide by it.

Date and Signature.....



Reference texts

<u>Legal text and regulations</u>	<u>References</u>
<u>Regulations relating to cryptographic measures.</u>	Executive Decree No. 16-61 of 02 Jumada El Oula 1437, corresponding to 11 February 2016, amending and supplementing Executive Decree No. 09-410 of 23 Dhou El-Hidja 1430, corresponding to 10 December 2009, establishing the security rules applicable to activities involving sensitive equipment.
<u>General rules relating to postal Services and Electronic Communications.</u>	Law No.18-04 of 24 Shaaban 1439, corresponding to 10 May 2018, setting out the rules relating to postal services and electronic communications
<u>Intellectual Property (Software)</u>	Ordinance No.03-05 of 19 Jumada El Oula 1424, corresponding to 19 July 2003, related to copyright and related rights
<u>Electronic Certification.</u>	Law No. 15-04 of Rbie Ethani 1436, corresponding to 1 February 2015, setting out the rules relating to electronic signatures and certifications. Decree. No.2016-134 of 17 Rajab 1437, corresponding to 25 April 2016, established the organization, operation and missions of technical and administrative services of the national electronic certification authority. Decree No. 2016-135 of 17 Rajab 1437, corresponding to 25 April 2016, laying down the nature, composition, organization and functioning of the governmental electronic certification authority.
<u>Protection of Personal Data.</u>	Law No. 18-07 of 25 Ramadan 1439, corresponding to 10 Juin 2018, concerning the protection of natural persons in the processing of personal data.

<u>Offences related to information and communication technologies (ICT).</u>	Law No.09-04 of 14 Shaaban 1430, corresponding to 05 August 2009, establishing specific rules regarding the prevention and combating of offences related to information and communication technologies.
<u>Combating Cybercrime</u>	Presidential Decree No. 14-252 of 13 Dhou El Kaada 1435, corresponding to 08 September 2014, ratifying the Arab Convention on Combating Cybercrime.



Setif 1 University - Ferhat ABBAS



Charte informatique De L'Université Sétif 1- Ferhat Abbas

Version 1.0

Edition 2024

Setif 1 University - Ferhat ABBAS

Cette charte informatique est modifiable et ajustable suivant les développements technologiques et les textes réglementaires en vigueur.

L'université Ferhat Abbas Sétif 1 met en œuvre un système d'information et de communication nécessaire au bon déroulement des activités académiques, pédagogiques, scientifiques et professionnelles, comprenant notamment un réseau informatique et téléphonique, logiciels, site et plateformes Web, messagerie, ainsi que des équipements informatiques fixes et mobiles.

L'utilisation du système d'information et de communication et des ressources informatiques doit être effectuée exclusivement à des fins académiques et professionnelles, sauf par exception autorisée par les services concernés.

Par ailleurs, des tiers à l'UFAS1 peuvent également avoir accès aux équipements informatiques et aux systèmes d'information et de communication de l'UFAS1.

La charte informatique vise à définir les règles et les droits d'utilisation de l'ensemble des moyens informatiques disponibles au sein des structures de l'Université Sétif 1- Ferhat Abbas, et à préciser les responsabilités des utilisateurs (enseignants, étudiants et ATS) afin de permettre un usage convenable et optimal des ressources informatiques disponibles, en garantissant un niveau minimal de sécurité adapté au milieu universitaire.

De même, cette charte vise également à sensibiliser les utilisateurs aux risques liés à l'intégrité et à la confidentialité des informations traitées et des ressources utilisées.

La charte est diffusée à l'ensemble des utilisateurs et ces derniers sont informés systématiquement de chaque mise à jour apportée. À ce titre, elle est systématiquement communiquée à tous les utilisateurs et disponible sur le site institutionnel de l'université.

Des actions de communication, d'information et de sensibilisation internes sont organisées régulièrement afin de maintenir un niveau d'information suffisant sur les bonnes pratiques recommandées.

1. Objectif

Cette charte a pour objectifs :

1.1 De sensibiliser les utilisateurs aux risques liés à la sécurité informatique en matière de libertés et de vie privée, notamment à travers les traitements de données à caractère personnel qu'ils sont amenés à effectuer.

1.2 D'informer les utilisateurs sur :

- Les usages permis des moyens informatiques mis à leur disposition ;
- Les règles de sécurité en vigueur ;
- Les mesures de contrôle prises par l'UFAS1 ;
- Les sanctions éventuellement encourues par les utilisateurs.

1.3 De formaliser les règles générales de sécurité que les utilisateurs s'engagent à respecter, en contrepartie de la mise à disposition des systèmes d'information et des équipements informatiques, et ainsi de déterminer les droits et devoirs des utilisateurs.

2. Définition de concepts

2.1 Ressources informatiques

Elles incluent tous les moyens matériels et logiciels, ainsi que l'accès au Web, à l'intranet et à la messagerie électronique, disponibles au sein de l'université ou accessibles de l'extérieur du campus.

On mentionne notamment les réseaux, les serveurs, les stations de travail, les logiciels, les applications, les sites et plateformes Web, les bases de données, les routeurs, les commutateurs, les points d'accès Wi-Fi, les câbles, les imprimantes et scanners, les téléphones IP, les disques durs et les disques flash, etc.

2.2 Propriété des ressources informatiques

Toutes les ressources informatiques fournies aux utilisateurs appartiennent exclusivement à l'université Ferhat Abbas - Sétif 1. De même, toutes les données stockées sur les équipements de l'université ou transitant dans ses réseaux sont la propriété exclusive de l'université.

2.3 Utilisateurs concernés

Les règles et droits d'accès sont applicables à tous les utilisateurs ayant un accès permanent ou temporaire aux ressources de l'université : enseignants, étudiants, doctorants, chercheurs, employés et agents administratifs et techniques, enseignants vacataires, stagiaires, invités, etc.

2.4 Services Internet

La mise à disposition par des serveurs locaux ou de moyens d'échanges et d'informations diverses : Web, messagerie, forum, téléphonie IP, visioconférence, etc.

3. Champs d'application

Les règles définies dans cette charte s'appliquent à tous les moyens informatiques proposés par l'université et à tous les utilisateurs de ces moyens dans tous les campus et toutes les structures de l'UFAS, à l'intérieur et à l'extérieur du campus

4. Droit d'accès aux ressources informatiques

4.1 L'accès pour chaque utilisateur est accordé dans la limite des prérogatives qui lui sont attribuées. Ce droit est personnel et ne peut être cédé, même temporairement, à un tiers. Il est matérialisé par la création d'identifiants nominatifs et confidentiels pour chaque utilisateur des ressources mises à disposition.

4.2 Le droit d'accès peut être limité ou retiré, par mesure conservatoire, si le comportement de l'utilisateur n'est pas en adéquation avec la présente charte.

4.3 Un utilisateur ne peut en aucun cas permettre à une autre personne d'accéder aux ressources de l'université au moyen de ses identifiants. Dans cette situation, l'utilisateur sera responsable des actions effectuées avec ses identifiants.

4.4 Toute perte, tout vol ou toute divulgation d'informations d'authentification doivent être immédiatement signalés à l'université.

5. Conditions d'utilisation

5.1 Les ressources informatiques mises à disposition par l'université ne peuvent être utilisées qu'à des fins professionnelles.

5.2 L'accès à une ressource informatique n'est permis qu'aux personnes dûment autorisées et identifiées de l'université. Des procédures d'autorisation préalable de la part de la structure responsable de la ressource en question peuvent être exigées pour des applications particulières.

5.3 Le droit d'accès est limité à des activités conformes de ladite structure et ne peut être utilisé dans d'autres activités hors du cadre défini.

6. Responsabilités de l'université

6.1 Mettre à disposition de l'utilisateur les ressources informatiques nécessaires à l'exécution des missions qui lui incombent.

6.2 Garantir le bon fonctionnement et la disponibilité des ressources informatiques.

6.3 Maintenir la qualité du service fourni aux utilisateurs dans la limite des moyens alloués.

6.4 Informer les utilisateurs des procédures et de la politique applicable en matière de ressources informatiques.

6.5 Mettre en œuvre les moyens nécessaires pour assurer la confidentialité et l'intégrité des documents et des échanges électroniques des utilisateurs.

6.6 Informer les utilisateurs que les activités sur le réseau et les systèmes font l'objet d'une surveillance automatisée.

6.7 Sensibiliser les utilisateurs aux risques liés à la sécurité informatique.

7. Responsabilité de l'utilisateur

7.1 Respecter les lois et les règlements en vigueur.

7.2 Respecter la présente charte ainsi que les différentes procédures et politiques de l'organisme.

7.3 Appliquer scrupuleusement les mesures et les directives de sécurité informatique de l'organisme.

7.4 Ne pas utiliser ou tenter d'utiliser les comptes d'autrui.

7.5 L'utilisateur est seul responsable de toute utilisation des moyens d'authentification mis à sa disposition par l'université.

7.6 En cas d'absence, même temporaire, il est impératif que l'utilisateur verrouille l'accès au matériel qui lui est confié ou à son propre matériel, dès lors que celui-ci contient des informations à caractère professionnel.

7.7 L'utilisateur doit effectuer des sauvegardes régulières des fichiers dont il dispose sur le matériel mis à sa disposition.

7.8 L'utilisateur doit éviter d'installer des logiciels, de copier ou d'installer des fichiers susceptibles de créer des risques de sécurité au sein de l'université.

7.9 L'utilisateur veille au respect de la confidentialité des informations en sa possession. Il doit en toutes circonstances veiller au respect de la législation, qui protège notamment les droits de propriété intellectuelle, le secret des correspondances, les données personnelles, les systèmes de traitement automatisé de données.

8. Règles de déontologie informatique

Chaque utilisateur s'engage à respecter les règles de la déontologie informatique et à ne pas effectuer intentionnellement des opérations qui pourraient avoir pour conséquences :

8.1 De masquer sa véritable identité.

8.2 De porter atteinte à l'image, à la réputation et à l'intégrité de l'université.

8.3 D'altérer, de modifier des données ou d'accéder à des informations appartenant à d'autres utilisateurs du réseau ou à l'université, sans leur consentement.

8.4 D'interrompre ou de perturber le fonctionnement normal du réseau ou d'un des systèmes connectés au réseau.

8.5 De modifier ou de détruire des informations sur un des systèmes.

8.6 De se connecter ou d'essayer de se connecter à un site sans y être autorisé.

8.7 De tenter d'intercepter des communications entre tiers.

9. Protection du poste de travail

9.1 Verrouiller l'accès au poste de travail en cas d'absence, même temporaire.

9.2 Alerter les services techniques en cas d'ouverture d'un nouvel équipement connecté au poste de travail.

9.3 S'assurer que son poste de travail dispose d'un antivirus et informer le service concerné de toute alerte de sécurité.

9.4 Ne jamais connecter des équipements personnels au poste de travail.

9.5 Scanner tous les supports amovibles connectés au poste de travail avant de les utiliser.

9.6 Éteindre l'ordinateur pendant les périodes d'inactivité prolongées (nuit, week-end, vacances, etc.)

9.7 Ne pas intervenir physiquement sur le matériel.

10. Messagerie électronique

10.1 L'utilisateur s'engage à ne pas partager les accès de son compte de messagerie fournis par l'université avec une autre personne.

10.2 L'utilisateur s'engage à avoir un mot de passe robuste : alphanumérique avec des caractères spéciaux et des majuscules, et à le modifier régulièrement.

10.3 L'adresse de messagerie ne peut être utilisée dans des sites qui peuvent présenter des risques de sécurité pour le compte de l'utilisateur ou les ressources de l'université.

10.4 Chaque utilisateur doit créer sa propre signature comportant ses informations de contact et l'utiliser dans chaque envoi de message.

10.5

Ne pas ouvrir des fichiers ou des liens transmis à partir d'adresses e-mail inconnues.

10.6 Chaque utilisateur doit organiser et mettre en œuvre les moyens nécessaires à la conservation des messages pouvant être indispensables.

10.7 L'utilisation et la gestion du compte de messagerie sont de la responsabilité de l'utilisateur.

10.8 Ne pas utiliser la messagerie à des fins personnelles ou partisans.

10.9 Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antivirus et d'un filtrage anti spam. Les utilisateurs sont invités à informer le centre des systèmes et des réseaux des dysfonctionnements qu'ils constatent dans le dispositif de filtrage.

10.10 L'envoi de messages électroniques à des tiers obéit aux mêmes règles que l'envoi de correspondances postales, en particulier en termes d'organisation hiérarchique. En cas de doute sur l'expéditeur compétent pour envoyer le message, il convient d'en référer au centre des systèmes et des réseaux.

10.11 Le risque de retard, de non-remise et de suppression automatique des messages électroniques doit être pris en considération pour l'envoi de correspondances importantes. Les messages importants sont envoyés avec un accusé de réception ou signés électroniquement.

10.12 Pour des raisons techniques, l'envoi de messages électroniques n'est possible, directement, que vers un nombre limité de destinataires fixé par le centre des systèmes et des réseaux. Cette limite est susceptible d'être levée temporairement sur demande.

10.13 De même, la taille, le nombre et le type des pièces jointes peuvent être limités par le centre des systèmes et des réseaux pour éviter l'engorgement du système de messagerie.

11. Internet, Intranet et connectivité

11.1 L'accès au Web via l'infrastructure de l'université est ouvert à des usages pédagogiques, de recherche et de gouvernance.

11.2 Ne pas utiliser ce service à des fins malveillantes, obscènes, frauduleuses, haineuses, diffamatoires ou illégales.

11.3 Tout téléchargement de fichiers, notamment de sons, d'images ou de vidéos, sur le Web doit s'effectuer dans le respect des droits de la propriété intellectuelle et ne doit pas sortir du cadre de l'activité académique, pédagogique, de recherche et de gouvernance.

11.4 Le téléchargement de fichiers vidéo, audio ou de logiciels de grandes tailles et qui peuvent générer une lenteur d'accès au Web pour les autres utilisateurs est strictement interdit.

11.5 Toute publication de pages d'informations ou de documents sur les sites Internet ou Intranet de l'UFAS doit être validée par un responsable de site ou responsable de publication nommément désigné.

11.6 L'utilisation du réseau ou d'un PC, serveur, modem, routeur ou autre équipement pour l'offre d'un service disponible depuis le Web comme RDP (Remote Desktop Protocol) est strictement interdite.

11.7 L'utilisateur ne doit pas usurper l'identité d'une autre personne et il ne doit pas intercepter de communications entre tiers.

11.8 L'utilisateur ne doit pas déposer des données sur un serveur interne ou ouvert au grand public (Google, Free, Orange, ...) ou sur le poste de travail d'un autre utilisateur sans y être autorisé par les responsables habilités.

11.9 L'utilisation d'Internet à des fins privées est tolérée dans des limites raisonnables et à condition que la navigation n'entrave pas l'accès professionnel.

11.10 L'insertion de points d'accès, modem, switch dans le réseau est soumise à l'autorisation préalable de l'ingénieur réseau.

13 Des appareils mobiles et des supports de stockage

L'utilisateur doit :

12.1 Signaler, à la hiérarchie dans l'immédiat, toute perte ou tout vol d'un appareil mobile ou d'un support de stockage professionnel.

12.2 Toujours verrouiller les appareils mobiles lorsqu'ils ne sont pas utilisés.

12.3 Désactiver les fonctions Wi-Fi et Bluetooth des appareils lorsque celles-ci ne sont pas nécessaires.

12.4 Interdiction formelle pour toute personne étrangère à l'université de transférer des documents par support amovible, tout échange de documents doit se faire par courriel. Dans le cas où le volume de données exige le recours à un support amovible, ce dernier doit être analysé par les services compétents avant toute utilisation.

12.5 Chiffrer les données confidentielles contenues dans des appareils mobiles et des supports de stockage.

12.6 Lors des déplacements professionnels, l'utilisateur doit garder ses appareils mobiles et supports de stockage amovibles sur soi.

13. Médias sociaux

13.1 Les comptes officiels doivent être gérés par des personnes désignées par l'université.

13.2 Toute publication doit être conforme aux valeurs et à l'image de l'université.

13.3 L'usage des réseaux sociaux durant le temps de travail doit rester limité à un usage professionnel.

13.4 Ne partagez pas d'informations confidentielles concernant l'université, ses membres ou ses activités sans autorisation.

13.5 Les opinions partagées en ligne doivent être les vôtres et ne pas engager la responsabilité de l'université, sauf autorisation explicite.

13.6 Respectez les droits d'auteur et la propriété intellectuelle lors du partage de contenus.

13.7 Signalez tout comportement inapproprié aux autorités compétentes de l'université.

14. Mesures de sécurité à appliquer lors des déplacements à l'étranger

14.1 Il est interdit d'utiliser des terminaux publics ou partagés pour accéder au compte de messagerie professionnelle ou aux applications métier.

14.2 Le missionnaire doit désactiver les fonctions de communication sans fil telles que le Wi-Fi et le Bluetooth des appareils lorsque celles-ci ne sont pas nécessaires.

14.3 Le missionnaire doit garder sur lui, en permanence, son terminal professionnel ainsi que les supports de stockage.

14.4 Le missionnaire doit supprimer toutes les données professionnelles sensibles, non nécessaires à la mission, de tous les supports amovibles avant tout déplacement à l'étranger.

14.5 Il doit informer la hiérarchie et la représentation diplomatique algérienne en cas d'inspection ou de saisie des équipements informatiques par des autorités étrangères lors des missions à l'étranger.

14.6 Il est interdit d'utiliser des équipements offerts lors d'un déplacement à l'étranger à des fins personnelles.

14.7 Il doit mentionner dans les comptes rendus de la mission la liste des objets connectés offerts lors du déplacement.

14.8 Il est formellement interdit qu'un transfert des documents par un étranger se fasse via des supports de stockage amovibles. Tout échange de documents doit se faire exclusivement par courriel.

14.9 Le missionnaire doit changer les mots de passe utilisés pendant la mission.

15. Sécurité

Les utilisateurs doivent veiller au respect strict des lois, réglementations et consignes de sécurité informatique en vigueur. Ils doivent notamment verrouiller leur poste de travail en cas d'absence, surtout en cas d'absence prolongée, s'interdire de connecter des équipements personnels, et disposer d'outils scanner et antivirus pour tous supports amovibles.

Les utilisateurs sont tenus de respecter les consignes suivantes :

15.1 Veiller à ne pas injecter des fichiers volumineux dans les réseaux informatiques.

15.2 Veiller à ne pas injecter des virus dans le réseau provenant de son flash disque, de sites Web malveillants ou de son compte de messagerie.

15.3 Bien vérifier les sites Web auxquels il accède et éviter les sites malveillants.

L'UFAS1 se réserve le droit de filtrer ou d'interdire l'accès à certains sites, de procéder au contrôle a priori ou a posteriori des sites visités et des durées d'accès correspondantes.

N.B. Un guide de bonne pratique lié à la sécurité informatique de l'UFAS1 a été établi et doit être respecté par tout utilisateur de ressources informatiques.

16. Cadre juridique

Les utilisateurs des ressources informatiques de l'université s'engagent à respecter les lois sur la propriété littéraire et artistique, ainsi que les lois qui lui sont associées sur la responsabilité civile, pénale et professionnelle. Ceci implique plus particulièrement le respect des obligations suivantes (sans que cela constitue une liste limitative) :

16.1 Le respect du droit d'auteur (droit moral, patrimonial, de diffusion).

16.2 Le respect de la vie privée ou du droit à l'image d'autrui.

16.3 L'interdiction de l'usurpation d'identité, du vol, de la diffamation, de la diffusion d'informations personnelles, confidentielles ou constituant une violation de la personnalité physique ou morale.

16.4 Le respect des exigences de la loi « Informatique et Libertés » (Loi n° 0317, Ordonnance n° 03-05 du 19 juillet 2003 : Protection des droits d'auteur et droits voisins et Loi n° 18-07 du 10 juin 2018 relative à la protection des personnes physiques dans le traitement des données à caractère personnel).

17. Confidentialité

17.1 Les données d'un utilisateur, sauf risque ou événement particulier, doivent être considérées comme privées si elles sont clairement identifiées comme telles. L'accès aux données privées d'un utilisateur exige l'accord de ce dernier.

17.2 Tout utilisateur autorisé à accéder aux données et aux ressources informatiques de l'Université s'engage à maintenir confidentielle l'information à laquelle il accède dans le cadre de ses fonctions.

17.3 L'accès à certains éléments du système d'information (comme la messagerie électronique ou téléphonique, les sessions sur les postes de travail, le réseau, certaines applications ou services interactifs) est protégé par des paramètres de connexion (identifiants, mots de passe).

17.4 Dans la mesure du possible, ces paramètres doivent être mémorisés par l'utilisateur et ne pas être conservés, sous quelque forme que ce soit. En tout état de cause, ils ne doivent pas être transmis à des tiers ou aisément accessibles. Ils

doivent être saisis par l'utilisateur à chaque accès et ne pas être conservés en mémoire dans le système d'information.

18. Gestion des incidents

En cas d'incident pouvant affecter la sécurité, l'université peut :

18.1 Déconnecter un utilisateur, avec ou sans préavis selon la gravité de la situation.

18.2 Isoler ou neutraliser provisoirement toute donnée ou fichier en contradiction avec la charte ou qui mettrait en péril la sécurité des systèmes d'information.

18.3 Prévenir le responsable hiérarchique.

19. Sanctions applicables

19.1 Le non-respect des règles définies dans la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des mesures disciplinaires proportionnelles à la gravité des faits constatés.

19.2 Sous réserve que soit informé le responsable hiérarchique, les responsables de la sécurité informatique peuvent avertir un utilisateur, limiter ou retirer provisoirement ses accès, et effacer ou compresser ou isoler toute donnée ou fichier en contradiction avec la charte ou qui mettrait en péril la sécurité des systèmes d'information.

19.3 Les cas de fraude, de non-respect des règles, les atteintes au bon fonctionnement de l'établissement sont soumis à la commission disciplinaire de l'UFAS1 qui prononce les sanctions.

20. Fin de la relation liant l'utilisateur à l'UFAS

20.1 Lorsque la relation liant l'utilisateur à l'université prend fin, l'utilisateur doit restituer à l'organisme toutes les ressources informatiques matérielles mises à sa disposition.

20.2 L'organisme procédera à la suppression de l'ensemble des ressources informatiques mises à sa disposition par l'organisme.

21. Entrée en vigueur de la charte

La présente charte prendra effet dès son adoption par les instances délibérantes de l'université : Conseil scientifique et Conseil d'administration.

Elle sera publiée par les moyens légaux de l'université et sera intégrée dans le règlement intérieur de l'UFAS.

22. Engagement individuel

Tous les membres de la famille universitaire, enseignants, étudiants, agents administratifs et techniques, doivent affirmer leur acceptation et engagement au respect de toutes les dispositions énoncées dans cette charte.

Ils doivent renseigner les champs d'information du cadre ci-dessous, apposer la mention « lu et accepté » et signer le document.



Je soussigné(e),

Nom et prénom :

Profession/Grade :

Faculté/Service :

Département :

Utilisateur des ressources informatiques et réseaux de l'Université Sétif 1-
Ferhat Abbas, certifie et affirme avoir pris connaissance de la présente charte
et m'engage à la respecter.

Date et signature :



Textes de références :

<u>Texte légal ou réglementation.</u>	<u>Références</u>
<u>Réglementation relative aux mesures cryptographiques.</u>	Décret exécutif n° 16-61 du 02 Joumada El Oula 1437 correspondant au 11 février 2016 modifiant et complétant le décret exécutif n° 09-410 du 23 Dhou ElHidja 1430 correspondant au 10 décembre 2009 fixant les règles de sécurité applicables aux activités portant sur les équipements sensibles.
<u>Les règles générales relatives à la poste et aux communications électroniques.</u>	Loi n° 18-04 du 24 Chaâbane 1439 correspondant au 10 mai 2018 fixant les règles générales relatives à la poste et aux communications électroniques.
<u>Propriété intellectuelle (les logiciels).</u>	Ordonnance n° 03-05 du 19 Joumada EL Oula 1424 correspondant au 19 juillet 2003 relative aux droits d'auteur et aux droits voisins.

<u>Certification électronique</u>	Loi n° 15-04 du 11 Rabie Ethani 1436 correspondant au 1er février 2015 fixant les règles générales relatives à la signature et à la certification électroniques. Décret n° 2016-134 du 17 Rajab 1437 correspondant au 25 avril 2016 fixant l'organisation, le fonctionnement et les missions des services techniques et administratifs de l'Autorité nationale de certification électronique. Décret n° 2016-135 du 17 Rajab 1437 correspondant au 25 avril 2016 fixant la nature, la composition, l'organisation et le fonctionnement de l'Autorité gouvernementale de certification électronique.
<u>Protection des données à caractère personnel.</u>	Loi n° 18-07 du 25 Ramadhan 1439 correspondant au 10 juin 2018 relative à la protection des personnes physiques dans le traitement des données à caractère personnel.
<u>Les infractions liées aux technologies de l'information et de la communication.</u>	Loi n° 09-04 du 14 Chaâbane 1430 correspondant au 05 août 2009 portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication.

Lutte contre la cybercriminalité.

**Décret présidentiel n° 14-252 du 13
Dhou El Kaada 1435
correspondant au 8 septembre 2014
portant ratification de la convention
arabe pour la lutte contre la
cybercriminalité.**



Setif 1 University - Ferhat ABBAS