

**ميثاق أمن تكنولوجيا المعلومات**

**الديباجة**

توفر اسم الهيئة للمستخدمين موارد تكنولوجيا المعلومات لتمكينهم من إنجاز المهام الموكلة إليهم،

الاستخدام غير السليم لهذه الوسائل يزيد من خطر تعريض أمن أنظمة المعلومات في المنظمة للخطر، كجزء من إنشاء الإطار الوطني لأمن المعلومات، مما تقرر وضع ميثاق لأمن تكنولوجيا المعلومات من أجل ضمان الحد الأدنى من الأمن.

**المادة** 1: **الغرض** من هذا الميثاق هو تحديد شروط وأحكام استخدام موارد تكنولوجيا المعلومات الخاصة بـــــــــــــ ـ"اسم الهيئة" . كما أنه يحدد قواعد الأمان التي يجب على المستخدمين احترامها.

**المادة** 2: **نطاق التطبيق** ينطبق هذا الميثاق على أي شخص لديه حق الوصول، بشكل دائم أو مؤقت، إلى موارد تكنولوجيا المعلومات الخاصة ب " اسم الهيئة "

**المادة** 3: **ملكية موارد تكنولوجيا المعلومات**

• جميع موارد تكنولوجيا المعلومات المتاحة للمستخدمين هي ملكية حصرية ل"اسم الهيئة" ؛

• جميع البيانات المستضافة على معدات "اسم الهيئة" أو التي تمر عبر شبكاتها هي ملكية حصرية للهيئة.

**المادة** 4: **شروط الوصول إلى الموارد وشبكة الكمبيوتر** أي وصول إلى موارد وشبكات الكمبيوتر الخاصة ب"اسم الهيئة" يخضع لإجراءات المصادقة المسبقة.

**المادة** 5: **مسؤولية المستخدم** يتحمل المستخدم وحده المسؤولية عن أي استخدام لوسائل المصادقة التي توفرها له "اسم الهيئة".

**المادة** 6: **حماية وسائل المصادقة** من أجل الحفاظ على وسائل المصادقة المتاحة له، يجب على المستخدم:

• ضمان حماية والحفاظ على معلومات المصادقة السرية الخاصة بها؛

• تغيير معلومات المصادقة السرية الخاصة به بشكل دوري؛ يُمنع منعًا باتًا توصيل معلومات المصادقة السرية الخاصة بك إلى أطراف ثالثة. MPT-DZ 2020 صفحة 79 من 89

**المادة** 7: استخدام موارد تكنولوجيا المعلومات

• لا يجوز استخدام موارد تكنولوجيا المعلومات الخاصة ب "اسم الهيئة" إلا للأغراض المهنية؛

• يجب على المستخدم الحفاظ على موارد تكنولوجيا المعلومات والوسائل المتاحة له؛

• لا يُسمح للمستخدم بتثبيت أو نشر التطبيقات أو البرامج على الوسائل أو موارد تكنولوجيا المعلومات المتاحة له؛

• في حالة تعطل هذه الوسائل أو الموارد، يجب عليه إبلاغ الهيكل المسؤول عن الصيانة على الفور.

**المادة** 8: **التزامات** "اسم الهيئة" ا**تجاه المستخدمين** يجب على "اسم الهيئة":

• إتاحة موارد تكنولوجيا المعلومات اللازمة للمستخدم لتنفيذ المهام الملقاة على عاتقه؛

• ضمان حسن سير العمل وتوافر موارد تكنولوجيا المعلومات؛

• الحفاظ على جودة الخدمة المقدمة للمستخدمين في حدود الموارد المخصصة؛

• إبلاغ المستخدمين بإجراءات وسياسات موارد تكنولوجيا المعلومات المعمول بها؛

• تنفيذ الوسائل اللازمة لضمان سرية وسلامة وثائق المستخدمين والتبادلات الإلكترونية؛

• إبلاغ المستخدمين بأن الأنشطة على الشبكة والأنظمة تخضع للمراقبة الآلية؛

• رفع وعي المستخدم بمخاطر أمن تكنولوجيا المعلومات.

**المادة** 9: **التزامات المستخدم** يجب على المستخدم:

• الامتثال للقوانين واللوائح المعمول بها؛

• احترام هذا الميثاق وكذلك الإجراءات والسياسات المختلفة "اسم الهيئة" ؛

• التطبيق الدقيق لتدابير وإرشادات أمن تكنولوجيا المعلومات الخاصة "اسم الهيئة" ؛

• لا تستخدم أو تحاول استخدام حسابات الآخرين؛

• الإبلاغ عن أي عملية مشبوهة أو حادث أمني دون تأخير.

**المادة** 10: **سلامة وحماية محطة العمل** يجب على المستخدم احترام تعليمات السلامة التالية بدقة.

• قفل الوصول إلى محطة العمل في حالة الغياب، ولو مؤقتًا؛ MPT-DZ 2020 صفحة 80 من 89.

• تنبيه الخدمات الفنية في حالة اكتشاف معدات جديدة متصلة بمحطة العمل؛

• تأكد من أن محطة العمل الخاصة بك بها برنامج مكافحة فيروسات، وأبلغ القسم المعني بأي تنبيهات أمنية؛

• لا تقم أبدًا بتوصيل المعدات الشخصية بمحطة العمل؛

• قم بمسح جميع الوسائط القابلة للإزالة المتصلة بمحطة العمل قبل استخدامها؛

• قم بإيقاف تشغيل الكمبيوتر خلال فترات عدم النشاط الطويلة (ليلة، عطلة نهاية الأسبوع، إجازة،)؛

• لا تتدخل فعليًا في المعدات (الوحدات المركزية المفتوحة، ...).

**المادة** 11: **استخدام الرسائل الإلكترونية المهنية** تزود "اسم الهيئة" المستخدمين بحسابات رسائل إلكترونية تسمح لهم بإرسال واستقبال رسائل إلكترونية ذات طبيعة مهنية.

لا يمكن استخدام الرسائل الاحترافية إلا لأغراض تجارية. ولهذا الغرض يمنع منعا باتا:

• استخدامه لأغراض شخصية أو حزبية؛

• استخدامه للتسجيل على الشبكات الاجتماعية والمنتديات والمواقع الإلكترونية؛

• فتح المرفقات و/أو الارتباطات التشعبية المرسلة من عناوين بريد إلكتروني غير معروفة؛

• افتح صندوق البريد الاحترافي من مناطق الوصول إلى الإنترنت المجتمعية، وخاصة مقاهي الإنترنت؛

عندما تتطلب مهام المستخدم التسجيل على الشبكات الاجتماعية أو المنتديات أو المواقع الإلكترونية، يتم تخصيص عنوان بريد إلكتروني مخصص لهذا الغرض له بعد الحصول على رأي إيجابي من السلطة المختصة. يجب على المستخدم توخي الحذر عند استخدام رسائل البريد الإلكتروني، والتأكد من ذلك:

• عنوان المستلم مصاغ بشكل جيد؛

• يحق للمستلم الوصول إلى المحتوى المرسل؛

• تم إرفاق المرفقات الصحيحة بالمستند.

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

**المادة** 12: **استخدام الإنترنت** يتعهد المستخدمون الذين لديهم إمكانية الوصول إلى الإنترنت بما يلي:

• لا تستخدم هذه الخدمة عمدًا لأغراض خبيثة أو فاحشة أو احتيالية أو بغيضة أو تشهيرية أو إباحية أو غير قانونية؛

• لا تقدم معلومات تتعلق بوظيفتها أو رتبتها أو مسؤوليتها على شبكات التواصل الاجتماعي؛ MPT-DZ 2020 صفحة 81 من 89

• لا تفرط في تحميل شبكة الجسم؛

• توخي الحذر عند تنزيل الملفات، وتأكد من فحصها باستخدام برنامج مكافحة الفيروسات.

**المادة** 13: **الأجهزة المحمولة ووسائط التخزين** يجب على المستخدم:

• الإبلاغ فورًا إلى التسلسل الهرمي عن أي فقدان أو سرقة لجهاز محمول أو وسيلة تخزين احترافية؛

• قم دائمًا بقفل الأجهزة المحمولة عندما لا تكون قيد الاستخدام؛

• تعطيل وظائف Wi-Fi وBluetooth للأجهزة عندما لا تكون ضرورية؛

• الحظر الرسمي على أي شخص خارج "اسم الهيئة" لنقل المستندات عن طريق الوسائط القابلة للإزالة، وأي تبادل للمستندات يجب أن يتم عن طريق البريد الإلكتروني. إذا كان

حجم البيانات يتطلب استخدام الوسائط القابلة للإزالة، فيجب تحليل هذه الأخيرة من قبل الخدمات المختصة قبل أي استخدام؛

• تشفير البيانات السرية الموجودة في الأجهزة المحمولة ووسائط التخزين؛

• عند السفر للعمل، يجب على المستخدم الاحتفاظ بأجهزته المحمولة ووسائط التخزين القابلة للإزالة معه.

**المادة** 14: **التدابير الأمنية الواجب تطبيقها عند السفر إلى الخارج**

• يُحظر استخدام المحطات العامة أو المشتركة (أجهزة الكمبيوتر والأجهزة اللوحية) للوصول إلى حساب البريد الإلكتروني الاحترافي أو تطبيقات الأعمال؛

• يجب على المبشر أن يحتفظ بمحطته المهنية ووسائط التخزين معه في جميع الأوقات؛

• يجب على المبشر تعطيل وظائف الاتصال اللاسلكي مثل Wi-Fi وBluetooth للأجهزة عندما لا يكون ذلك ضروريًا؛

• يجب على المبشر حذف جميع البيانات المهنية الحساسة، غير الضرورية للمهمة، من جميع الوسائط القابلة للإزالة قبل أي سفر إلى الخارج؛

• يجب على المبشر إبلاغ التسلسل الهرمي والتمثيل الدبلوماسي الجزائري في حالة التفتيش أو مصادرة أجهزة الكمبيوتر من قبل السلطات الأجنبية أثناء البعثات في الخارج؛

• يحظر استخدام المعدات المقدمة عند السفر إلى الخارج لأغراض مهنية؛

• يجب على المبشر أن يذكر في تقارير البعثة قائمة الأشياء المتصلة المقدمة أثناء الرحلة؛

MPT-DZ 2020 صفحة 82 من 89

• يمنع منعا باتا أن يتم نقل المستندات من قبل أجنبي عبر وسائط تخزين قابلة للإزالة. يجب أن يتم أي تبادل للمستندات حصريًا عبر البريد الإلكتروني؛

• يجب على المبشر تغيير كلمات المرور المستخدمة أثناء المهمة.

**المادة** 15: **نهاية العلاقة التي تربط المستخدم** "اسم الهيئة".

• عندما تنتهي العلاقة بين المستخدم والمؤسسة، يجب على المستخدم أن يعيد إلى المؤسسة جميع موارد الحوسبة المادية المتاحة له؛

• ستقوم "اسم الهيئة" بحذف كل الوصول المنطقي للمستخدم إلى موارد تكنولوجيا المعلومات التي توفرها له.

**المادة** 16: **إدارة الحوادث** في حالة وقوع حادث يمكن أن يؤثر على الأمن، يجوز "اسم الهيئة":

• قطع الاتصال المستخدم، مع أو بدون إشعار حسب خطورة الموقف؛

• عزل أو تحييد أي بيانات أو ملف يتعارض مع الميثاق أو من شأنه أن يعرض أمن نظم المعلومات للخطر مؤقتًا؛

• إخطار المسؤول المباشر.

**المادة** 17: **عدم الالتزام بالميثاق** من المرجح أن يؤدي عدم الالتزام بالقواعد المحددة في هذا الميثاق إلى تحمل مسؤولية المستخدم ويؤدي إلى اتخاذ إجراءات تأديبية ضده تتناسب مع خطورة الوقائع الملاحظة.

شريطة إبلاغ المسؤول المباشر، يجوز لمديري أمن تكنولوجيا المعلومات:

• إخطار المستخدم؛

• تقييد وصول المستخدم أو إزالته مؤقتًا؛

• مسح أو ضغط أو عزل أي بيانات أو ملف يتعارض مع الميثاق أو من شأنه أن يعرض أمن نظم المعلومات للخطر.

مع عدم الإخلال بالعقوبات التأديبية، يجوز أن يخضع المخالف لأحكام هذا الميثاق لإجراءات قانونية.

**المادة** 18: **الدخول حيز التنفيذ**

يدخل هذا الميثاق حيز التنفيذ عند توقيع المستخدم.

أي رفض للتوقيع سيمنع المستخدم من الوصول إلى موارد تكنولوجيا المعلومات الخاصة بالمؤسسة.