سياسة الاستخدام المقبول

للإنترنت والأنظمة والتقنيات الحكومية

للجهات الحكومية في ليبيا

أعدّت هذه المسودة:

مجموعة العمل المتخصصة في إعادة صياغة السياسات العامة الرقمية

بقيادة مبادرة أنير بالتعاون مع مجتمع الإنترنت - ليبيا

مشروع اصلاح السياسات الرقمية في ليبيا

مارس 2026

وثيقة عمل للمشاورة العامة — غير رسمية

أولاً: الغرض والنطاق

تحدد هذه السياسة الاستخدامات المسموح بها وغير المسموح بها للإنترنت والأنظمة المعلوماتية والأجهزة والشبكات المملوكة للجهات الحكومية الليبية أو المدارة من قِبلها. تسري هذه السياسة على جميع موظفي الجهات الحكومية والمتعاقدين والاستشاريين وكل من يستخدم الموارد التقنية الحكومية بصفة مؤقتة أو دائمة.

ثانياً: المبادئ الأساسية

المشروعية: يجب أن يكون كل استخدام للموارد الرقمية الحكومية متسقاً مع التشريعات الليبية النافذة والسياسات الداخلية المعتمدة.

الغرضية: تُستخدم الموارد الرقمية الحكومية أساساً لأغراض العمل الرسمي، ويُسمح بالاستخدام الشخصي المحدود بشرط ألا يتعارض مع المصالح الحكومية.

المساءلة: كل مستخدم مسؤول مسؤولية شخصية عن الاستخدام الذي يجريه بحسابه الرسمي أو من جهازه الحكومي.

الأمن: لا يجوز إجراء أي استخدام من شأنه تعريض أمن الأنظمة أو البيانات الحكومية أو بيانات المواطنين للخطر.

ثالثاً: الاستخدامات المسموح بها

3-1 الاستخدام الرسمي

1. التواصل الرسمي عبر البريد الإلكتروني الحكومي في شؤون العمل.
2. الوصول إلى قواعد البيانات والأنظمة الحكومية لأداء المهام الرسمية.
3. البحث والاطلاع على المعلومات اللازمة لأداء المهام الوظيفية.
4. المشاركة في برامج التدريب والتطوير الإلكترونية المعتمدة.
5. استخدام الأنظمة المعتمدة من قِبل الجهة للتنسيق والتعاون مع الجهات الأخرى.

3-2 الاستخدام الشخصي المحدود المسموح به

1. الاستخدام الشخصي المحدود للإنترنت خلال أوقات الراحة الرسمية بشرط ألا يؤثر في الإنتاجية.
2. التواصل الشخصي العرضي شريطة الالتزام بجميع قواعد هذه السياسة.

رابعاً: الاستخدامات المحظورة

4-1 المحظورات المطلقة

- الوصول إلى المحتوى الذي يتعارض مع القوانين الليبية النافذة.
- تحميل أو تثبيت برمجيات غير مرخصة أو غير معتمدة على الأجهزة الحكومية.
- الكشف عن معلومات حكومية سرية أو بيانات مواطنين لجهات غير مخوَّلة.
- استخدام الأنظمة الحكومية لمهاجمة أنظمة أخرى أو نشر برمجيات خبيثة.
- انتحال هوية موظف آخر أو التلاعب بسجلات الاستخدام.
- استخدام الموارد الحكومية لأغراض تجارية شخصية أو سياسية حزبية.
- تجاوز إجراءات الأمن المعتمدة أو التحايل على أنظمة الحماية والجدران النارية.
- تشغيل برامج التنقيب أو استخراج البيانات الضخمة دون إذن مسبق.

خامساً: مراقبة الاستخدام

تحتفظ الجهة الحكومية بحق مراقبة استخدام الأنظمة والشبكات الحكومية للتحقق من الامتثال لهذه السياسة. وتُجرى المراقبة وفق الضوابط الآتية:

1. تُجرى مراقبة الاستخدام بصفة منتظمة وعشوائية ولا تستهدف موظفاً بعينه دون مسوّغ.
2. يُخطَر الموظفون بوجود أنظمة المراقبة وطبيعتها عند التعيين وعند التحديث.
3. لا تُستخدم نتائج المراقبة لأغراض غير تلك المتعلقة بأمن الأنظمة والامتثال للسياسة.
4. لا تمتد المراقبة إلى المحتوى الشخصي للاتصالات إلا بأمر قضائي.
5. تُحتفظ بسجلات المراقبة لمدة لا تتجاوز سنة واحدة ما لم تستدعِ تحقيقات قائمة غير ذلك.

سادساً: المخالفات والعقوبات

تُصنَّف مخالفات هذه السياسة على ثلاث درجات:

المخالفات البسيطة: استخدام شخصي مفرط، تحميل محتوى غير ملائم — العقوبة: تحذير خطي وإعادة التدريب.

المخالفات المتوسطة: تثبيت برمجيات غير مرخصة، مشاركة كلمات المرور، تجاوز قيود الشبكة — العقوبة: توقيف مؤقت عن العمل أو خصم من الراتب.

المخالفات الجسيمة: الإفصاح عن بيانات سرية، مهاجمة الأنظمة، الاحتيال الإلكتروني — العقوبة: الإحالة للتأديب وربما الإحالة للقضاء.

سابعاً: الالتزامات والمراجعة

1. يوقّع كل موظف على نموذج التزام بهذه السياسة عند التعيين وعند كل مراجعة سنوية.
2. تُراجَع هذه السياسة سنوياً وتُحدَّث عند الحاجة.
3. يُقدَّم تقرير سنوي للإدارة العليا عن حوادث المخالفات وإجراءات التصحيح.

سياسة حماية البيانات والخصوصية

لبيانات المواطنين في الجهات الحكومية

أعدّت هذه المسودة:
مجموعة العمل المتخصصة في إعادة صياغة السياسات العامة الرقمية
بقيادة مبادرة أنير بالتعاون مع مجتمع الإنترنت - ليبيا
مشروع اصلاح السياسات الرقمية في ليبيا

مارس 2026

وثيقة عمل للمشاورة العامة — غير رسمية

أولاً: الغرض والنطاق

تحدد هذه السياسة الإطار الداخلي للجهات الحكومية الليبية في جمع بيانات المواطنين ومعالجتها وتخزينها ومشاركتها والاحتفاظ بها والتخلص منها. وتستند هذه السياسة إلى أحكام قانون حماية البيانات الشخصية النافذ وتُكملها على المستوى التنفيذي الداخلي. تسري على جميع أقسام الجهة وموظفيها ومتعاقديها الذين يتعاملون مع بيانات المواطنين.

ثانياً: مبادئ معالجة البيانات

المشروعية: لا تُجمع البيانات ولا تُعالج إلا لغرض رسمي محدد مستند إلى صلاحية قانونية أو موافقة صريحة.

الحد الأدنى: لا تُجمع إلا البيانات الضرورية للغرض المحدد، ويُحظر جمع بيانات احتياطية أو تجميعية.

الدقة: تُتخذ خطوات فعلية للتحقق من صحة البيانات وتحديثها ومعالجة طلبات التصحيح.

التحديد الزمني: لا تُحتفظ بالبيانات أطول مما تقتضيه الحاجة الرسمية الموثقة.

الأمن: تُطبَّق تدابير تقنية وتنظيمية ملائمة لحماية البيانات من الوصول غير المصرح به أو الفقدان أو الإتلاف.

ثالثاً: تصنيف البيانات

3-1 مستويات التصنيف

عام: بيانات يمكن الإفصاح عنها للجمهور دون قيد.

داخلي: بيانات للاستخدام الداخلي فقط لا تُشارَك خارج الجهة إلا بموجب اتفاقية.

سري: بيانات شخصية للمواطنين تستوجب حماية مشددة ولا تُشارَك إلا بموجب صلاحية قانونية.

سري للغاية: بيانات حساسة كالسجلات الصحية والمعتقدات وبيانات الأمن — تستوجب أعلى مستوى من الحماية.

3-2 قواعد التعامل مع كل مستوى

1. البيانات السرية والسرية للغاية: يُقيَّد الوصول على أساس الحاجة للمعرفة فقط، ويُسجَّل كل وصول إليها.
2. يُحظر تخزين البيانات السرية على أجهزة شخصية أو خدمات سحابية غير معتمدة.
3. تُشفَّر البيانات السرية والسرية للغاية أثناء النقل وأثناء التخزين.
4. لا يجوز طباعة البيانات السرية إلا لضرورة موثقة، وتُتلف المطبوعات بالتقطيع الآمن.

رابعاً: حقوق المواطنين وآليات تطبيقها

تلتزم الجهة بضمان حقوق المواطنين الآتية المستمدة من قانون حماية البيانات الشخصية:

1. حق الاطلاع: للمواطن معرفة ما تحتفظ به الجهة من بياناته.
2. حق التصحيح: للمواطن طلب تصحيح بياناته غير الدقيقة خلال ثلاثين يوماً من الطلب.

3. حق الاعتراض: للمواطن الاعتراض على استخدام بياناته لأغراض غير ضرورية.
4. حق المسح: في الحالات المنصوص عليها في قانون حماية البيانات الشخصية.

تُعيّن كل جهة موظفاً مسؤولاً عن خصوصية البيانات، وتوفر آلية سهلة لتلقي طلبات المواطنين والرد عليها خلال المدد القانونية.

خامساً: مشاركة البيانات مع جهات أخرى

لا تُشارَك البيانات الشخصية للمواطنين مع جهات حكومية أخرى أو خاصة أو دولية إلا وفق الشروط الآتية:

1. وجود مسوّغ قانوني صريح أو موافقة من صاحب البيانات.
2. إبرام اتفاقية مشاركة بيانات تحدد الغرض ونطاق البيانات المشتركة ومتطلبات الأمن ومدة الاحتفاظ.
3. تسجيل كل عملية مشاركة في سجل المعالجة.
4. الحصول على موافقة مدير الجهة أو من يفوّضه قبل أي مشاركة واسعة النطاق.

سادساً: إدارة انتهاكات البيانات

1. يُبلَّغ مسؤول الخصوصية فوراً بأي انتهاك فعلي أو مشتبه به للبيانات.
2. تُقيَّم خطورة الانتهاك خلال ساعة واحدة من الإبلاغ.
3. تُخطَر هيئة حماية البيانات الشخصية خلال اثنتين وسبعين ساعة من اكتشاف الانتهاك.
4. يُخطَر المواطنون المتضررون في أسرع وقت ممكن إذا كان الانتهاك يشكّل خطراً على حقوقهم.
5. يُوثَّق كل انتهاك بتفاصيله وإجراءات المعالجة في سجل الحوادث الأمنية.

سابعاً: الاحتفاظ بالبيانات والتخلص منها

تُعدّ كل جهة جدول احتفاظ بالبيانات يحدد مدة الاحتفاظ بكل فئة من البيانات بناءً على:

1. المتطلبات القانونية والتنظيمية النافذة.
2. الاحتياجات التشغيلية الموثقة.
3. الالتزامات الأرشيفية الوطنية.

عند انتهاء مدة الاحتفاظ، تُتلف البيانات الرقمية بطرق آمنة موثقة، وتُتلف المطبوعات بالتقطيع الآمن. ويُحتفظ بسجل بعمليات الإتلاف.

سياسة الأمن المعلوماتي

للجهات الحكومية الليبية

للجهات الحكومية في ليبيا

أعدّت هذه المسودة:

مجموعة العمل المتخصصة في إعادة صياغة السياسات العامة الرقمية

بقيادة مبادرة أنير بالتعاون مع مجتمع الإنترنت - ليبيا

مشروع اصلاح السياسات الرقمية في ليبيا

مارس 2026

وثيقة عمل للمشاورة العامة — غير رسمية

أولاً: الغرض والنطاق

تُرسي هذه السياسة الإطار الأمني الداخلي للجهات الحكومية الليبية لحماية أنظمتها المعلوماتية وشبكاتها وبياناتها من التهديدات الإلكترونية والمخاطر التقنية والبشرية. وتستند إلى الاستراتيجية الوطنية للأمن السيبراني وقانون الجرائم الإلكترونية النافذين.

ثانياً: إدارة المخاطر الأمنية

تلتزم كل جهة حكومية بـ:

1. إجراء تقييم شامل للمخاطر الأمنية مرة واحدة على الأقل سنوياً أو عند إجراء تغييرات جوهرية في الأنظمة.
2. الاحتفاظ بسجل المخاطر المحدَّث الذي يشمل تصنيف كل خطر وخطة معالجته.
3. إعداد خطة استمرارية أعمال وخطة تعافٍ من الكوارث واختبارهما سنوياً.
4. الإبلاغ الفوري للهيئة الوطنية لأمن وسلامة المعلومات عن الحوادث الأمنية الجسيمة.

ثالثاً: إدارة الهوية وصلاحيات الوصول

3-1 إنشاء الحسابات وإدارتها

1. يُنشأ حساب رسمي منفصل لكل موظف بهوية فريدة لا تُشارَك.
2. تُمنح الصلاحيات على أساس الحد الأدنى اللازم للعمل (مبدأ الامتياز الأدنى).
3. تُراجَع صلاحيات الوصول ربع سنوياً وتُحذف الصلاحيات الزائدة.
4. يُغلَق الحساب فوراً عند انتهاء خدمة الموظف أو نقله.

3-2 متطلبات كلمات المرور والمصادقة

1. تتألف كلمة المرور من اثني عشر حرفاً على الأقل تجمع حروفاً وأرقاماً ورموزاً.
2. لا تُعاد استخدام كلمات المرور السابقة الاثنتا عشرة.
3. تُفعَّل المصادقة الثنائية على جميع الحسابات التي تصل إلى البيانات السرية.
4. يُنتهي الجلسة تلقائياً بعد خمس عشرة دقيقة من عدم النشاط في الأنظمة الحساسة.

رابعاً: أمن الشبكة والأجهزة

1. تُطبَّق جدران نارية وأنظمة كشف التسلل على جميع نقاط الاتصال بالشبكة.
2. تُعزَل شبكات الضيوف والمقاولين الخارجيين عن الشبكة الداخلية.
3. لا تُوصَل الأجهزة الشخصية بالشبكة الداخلية إلا عبر بروتوكول آمن معتمد.

4. يُطبَّق تشفير القرص الصلب على جميع الأجهزة المحمولة التي تحمل بيانات حكومية.
5. تُحدَّث أنظمة التشغيل والتطبيقات بصفة منتظمة ولا يُتأخر في تطبيق تحديثات الأمن.
6. يُعطَّل كل منفذ USB أو وسيلة تخزين خارجية غير ضرورية للعمل.

خامساً: تشفير البيانات

تلتزم الجهة بتطبيق التشفير وفق الضوابط الآتية:

1. تُشفَّر جميع البيانات السرية والسرية للغاية أثناء التخزين وأثناء النقل.
2. تُستخدم خوارزميات تشفير معيارية معتمدة دولياً ولا تُستخدم خوارزميات مملوكة أو غير موثقة.
3. يُحتفظ بمفاتيح التشفير في مستودع آمن منفصل عن البيانات المشفرة.
4. يُجرى تدقيق دوري على فاعلية ممارسات التشفير.

سادساً: النسخ الاحتياطي والتعافي

1. تُجرى نسخ احتياطية يومية تلقائية للبيانات الحيوية.
2. تُخزَّن نسخة احتياطية واحدة على الأقل خارج الموقع الأصلي في مكان آمن.
3. يُختبَر استرداد البيانات من النسخ الاحتياطية ربع سنوياً ويُوثَّق الاختبار.
4. يُحدَّد الهدف الأقصى لاسترداد البيانات (RPO) وزمن الاسترداد (RTO) لكل نظام حيوي.

سابعاً: التوعية والتدريب الأمني

1. يخضع جميع الموظفين لتدريب أمن المعلومات عند التعيين وبصفة سنوية.
2. يُجرى اختبار محاكاة للتصيد الإلكتروني (Phishing) دورياً لقياس يقظة الموظفين.
3. يحصل الموظفون المنخرطون في إدارة الأنظمة الحيوية على تدريب متخصص وشهادات احترافية.
4. يُعقَد مع الموظفين تدريب خاص عند اكتشاف أساليب هجوم جديدة.

ثامناً: إدارة الحوادث الأمنية

تتبع كل جهة الإجراءات الآتية عند وقوع حادثة أمنية:

المرحلة 1 - الاكتشاف والإبلاغ: الإبلاغ الفوري لمسؤول الأمن المعلوماتي خلال ساعة من الاكتشاف.

المرحلة 2 - الاحتواء: عزل الأنظمة المتضررة لمنع انتشار الحادثة دون حذف الأدلة.

المرحلة 3 - الاستئصال: تحديد السبب الجذري وإزالته بالتنسيق مع الهيئة الوطنية لأمن وسلامة المعلومات.

المرحلة 4 - الاسترداد: استعادة الأنظمة المتضررة من نسخ احتياطية موثوقة واختبار سلامتها.

المرحلة 5 - التقييم: إعداد تقرير ما بعد الحادثة وتحديث إجراءات الأمن وفق الدروس المستفادة.

سياسة الشفافية والإفصاح الرقمي

للجهات الحكومية الليبية

للجهات الحكومية في ليبيا

أعدّت هذه المسودة:

مجموعة العمل المتخصصة في إعادة صياغة السياسات العامة الرقمية

بقيادة مبادرة أنير بالتعاون مع مجتمع الإنترنت - ليبيا

مشروع اصلاح السياسات الرقمية في ليبيا

مارس 2026

وثيقة عمل للمشاورة العامة — غير رسمية

أولاً: الغرض والنطاق

تُحدد هذه السياسة التزامات الجهات الحكومية الليبية في مجال الشفافية والإفصاح الرقمي تنفيذاً لأحكام قانون حرية المعلومات النافذ ومبادئ الحوكمة الرشيدة. تسري على جميع الجهات الحكومية المركزية والمحلية والهيئات العامة والشركات المملوكة للدولة.

ثانياً: التزامات الإفصاح الاستباقي

2-1 المعلومات الواجب نشرها دورياً

تنشر كل جهة حكومية على موقعها الإلكتروني الرسمي المعلومات الآتية ضمن الجداول الزمنية المحددة:

فورياً: القرارات والمراسيم والقوانين والتعميمات الصادرة.

شهرياً: بيانات الإنفاق والمشتريات والعقود التي تتجاوز قيمتها الحد المحدد.

ربع سنوياً: تقارير الأداء المؤسسي ومؤشرات الخدمة وتقارير الشكاوى.

سنوياً: الميزانية والتقرير المالي المدقق وتقرير الإنجازات وخطة العمل القادمة.

2-2 معايير الإفصاح

1. تُنشر المعلومات بصيغ رقمية قابلة للقراءة الآلية كلما أمكن (CSV, JSON, XML).
2. تُرفق بكل مجموعة بيانات وصف واضح للمحتوى والمنهجية ومصدر البيانات وتاريخ آخر تحديث.
3. تُتاح البيانات بترخيص مفتوح يسمح بإعادة استخدامها.
4. يُحدَّث الموقع الإلكتروني الرسمي بصفة منتظمة ولا يُسمح بوجود معلومات منتهية الصلاحية دون إشارة واضحة.
5. تُوفَّر نسخة ورقية أو طباعية من المعلومات للمواطنين في مراكز خدمة الجمهور.

ثالثاً: إدارة طلبات المعلومات

وفاءً بالتزامات قانون حرية المعلومات تلتزم كل جهة بـ:

1. تعيين مسؤول المعلومات ونشر بياناته علناً.
2. توفير نموذج إلكتروني وورقي موحد لتقديم طلبات المعلومات.
3. الرد على الطلبات خلال خمسة عشر يوم عمل من الاستلام.
4. إبلاغ الطالب بالتأخر المبرر خلال المدة الأصلية.
5. الاحتفاظ بسجل محوسب لجميع الطلبات الواردة ومآلاتها ونشر إحصاءاتها سنوياً.
6. عدم اشتراط تقديم الطالب أي مسوّغ لطلبه.

رابعاً: سياسة الموقع الإلكتروني الحكومي

4-1 متطلبات الموقع الإلكتروني

1. يكون لكل جهة موقع إلكتروني رسمي واحد يحمل النطاق الحكومي المعتمد (.gov.ly).
2. يتوافق الموقع مع معايير الإتاحة الرقمية لذوي الإعاقة (WCAG 2.1 مستوى AA).
3. يوفر الموقع محتوى باللغة العربية أساساً مع إمكانية توفير ترجمات.
4. يُختبَر الموقع أمنياً سنوياً ويُعالَج الثغرات المكتشفة خلال مدة محددة.
5. لا تُجمَع بيانات المستخدمين إلا بالحد الأدنى الضروري وبإشعار واضح.

4-2 إدارة المحتوى

1. تُعيَّن إدارة المحتوى لموظف مسؤول أو فريق محدد.
2. يُراجَع المحتوى دورياً وتُحذف المعلومات المنتهية الصلاحية أو تُعلَّم بوضوح.
3. تُحتفظ بنسخ أرشيفية من المحتوى المحذوف لمدة لا تقل عن خمس سنوات.

خامساً: الشفافية في المشتريات والعقود

تنشر كل جهة حكومية للعموم المعلومات الآتية المتعلقة بمشترياتها وعقودها:

1. إعلانات المناقصات والمزايدات العامة كاملةً قبل إغلاق باب التقديم.
2. نتائج المناقصات وأسماء الفائزين والقيم العقدية خلال ثلاثين يوماً من الترسية.
3. ملخصات العقود الموقعة التي تتجاوز قيمتها حداً تحدده اللوائح التنفيذية.
4. تقارير الأداء الدورية للعقود الكبرى.
5. معلومات التعديلات العقدية والمبالغ الإضافية.

سادساً: الشفافية في أداء الخدمات

1. تُنشَر ميثاق خدمات المواطن لكل جهة وتُحدَّث سنوياً وتتضمن مؤشرات الأداء المستهدفة.
2. تُنشر بصفة ربع سنوية مؤشرات الأداء الفعلي مقارنةً بالمستهدفة.
3. تُتاح إحصاءات الشكاوى المقدمة وأوقات المعالجة ومعدلات الرضا.
4. لا تُغلق قنوات الشكاوى ولا تُقيَّد إلا لأسباب تقنية موثقة ومؤقتة.

سابعاً: تقرير الشفافية السنوي

تُصدر كل جهة تقريراً سنوياً للشفافية يتضمن:

1. عدد طلبات المعلومات الواردة ونسبة الموافقة والرفض وأسباب الرفض الرئيسية.
2. عدد الطعون المقدمة ونتائجها.
3. تقييماً ذاتياً للامتثال لقانون حرية المعلومات.
4. خطة تحسين الشفافية للعام القادم.

تُرفع هذه التقارير إلى مفوضية حرية المعلومات وتُنشر علناً.

ثامناً: المراجعة والمساءلة

1. تُجري مفوضية حرية المعلومات تدقيقاً سنوياً على امتثال الجهات لهذه السياسة.
2. تُدرج نتائج التدقيق في التقرير السنوي العام للمفوضية.
3. تُصنَّف الجهات الحكومية سنوياً وفق مؤشر الشفافية الرقمية الوطني.
4. تُراجَع هذه السياسة كل سنتين لمواكبة التطورات التقنية والتشريعية.

ملاحظة ختامية

أُعدّت هذه السياسات الأربع في إطار مشروع اصلاح السياسات الرقمية في ليبيا، استناداً إلى التشريعات الأربعة التي أُعدّت في المرحلة ذاتها، وإلى توصيات مجموعات العمل متعددة الأطراف. هذه وثائق عمل مفتوحة للمشاورة العامة ومرحّب بالملاحظات عليها عبر: salam@annir.ly