وقف داركم

سياسة تقنية المعلومات/الأمن السيبراني

(IT & Cybersecurity Policy)

الرمز: DW-POL-IT | الإصدار: 1.0

تاريخ الإصدار: 05-02-2026

الرمز	DW-POL-IT
الإصدار	1.0
تاريخ السريان	2026/02/15
الجهة المالكة	الإدارة التنفيذية (COO) + مسؤول تقنية المعلومات/الأمن السيبراني (إن وجد)
جهة الاعتماد	مجلس الإدارة
جهات ذات علاقة	حماية البيانات/الامتثال | الموارد البشرية | إدارة البرامج/الحالات | المالية | المشتريات/العقود | المراجعة الداخلية | لجنة المخاطر
مرجع السياسات	DW-POL-DATA | DW-POL-HR | DW-POL-PRG | DW-POL-PRC | DW-POL-FIN | DW-POL-WHB | DW-POL-EXC | سياسة المخاطر
مستوى السرية	داخلي
دورية المراجعة	سنوياً أو عند الحاجة أو عند وقوع حادث جسيم

1) الهدف

- حماية أنظمة الوقف وبياناته (وخاصة بيانات المستفيدين الحساسة) من التهديدات السيبرانية والاختراقات وفقدان البيانات.
- تحديد ضوابط أساسية قابلة للتطبيق فوراً (Baseline Controls) حتى في حال عدم وجود فريق تقنية معلومات متفرغ.
- ضمان استمرارية الأعمال واستعادة الخدمات عند الأعطال أو الحوادث (BCP/DR) وربط ذلك بإدارة المخاطر.
- تحقيق قابلية التدقيق عبر سجلات واضحة (وصول/نسخ احتياطي/تحديثات/حوادث).

2) النطاق

- تشمل جميع الأصول التقنية: أجهزة الحاسب والهواتف، البريد الإلكتروني، حسابات السحابة، المواقع، الأنظمة (CRM/ERP/ملفات)، الشبكات، ووسائط التخزين.
- تنطبق على جميع المستخدمين: موظفين، متطوعين، متعاونين، مزودين لديهم وصول للأنظمة أو البيانات.
- تشمل البيانات المتداولة داخل وخارج الوقف (مستفيدين، متبرعين، موردين، موظفين).

3) تعريفات

المصطلح	التعريف
الأصل التقني	أي جهاز/حساب/نظام/خدمة أو ملف رقمي يمتلكه أو يستخدمه الوقف.
حساب مميز (Privileged)	حساب يمتلك صلاحيات إدارية عالية (مثل Admin/Owner).
حادث سيبراني	أي حدث يهدد سرية/سلامة/توافر البيانات أو الأنظمة (اختراق/تسريب/برمجيات خبيثة/فدية...إلخ).
نسخ احتياطي	نسخة محفوظة لاستعادة البيانات بعد فقدها/تلفها/تشفيرها.
MFA	المصادقة متعددة العوامل (رمز/تطبيق) إضافة لكلمة المرور.

4) مبادئ حاكمة

- الحد الأدنى من الصلاحيات: منح صلاحيات حسب الحاجة فقط (Least Privilege).
- المصادقة القوية: MFA إلزامي للحسابات الحساسة وحسابات الإدارة.
- الفصل بين الحسابات: حساب إداري منفصل عن حساب المستخدم اليومي عند الحاجة.
- التشفير وحماية الأجهزة: تشفير الأجهزة المحمولة وإقفالها تلقائياً.
- قابلية الاستعادة: نسخ احتياطي دوري مع اختبار استعادة.
- التبليغ السريع: أي حادثة تُبلّغ فوراً وفق مسار حوادث تقنية المعلومات والبيانات.

5) الحوكمة والأدوار والمسؤوليات

الجهة/الدور	المهام الأساسية
مجلس الإدارة	اعتماد السياسة، متابعة حوادث جسيمة وتقارير المخاطر، دعم موارد الأمن السيبراني عند الحاجة.
لجنة المخاطر	متابعة المخاطر التقنية (Cyber Risk)، مراجعة الحوادث الجوهرية، التوصية بإجراءات تصحيح.
حماية البيانات/الامتثال	تصنيف البيانات، ضبط القنوات المسموح بها، إدارة حوادث البيانات بالتنسيق مع IT.
COO	اعتماد التشغيل، ضمان تنفيذ الضوابط الأساسية، التصعيد للمجلس في الحوادث الجوهرية.
مسؤول IT/أمن سيبراني (إن وجد)	إدارة الأصول، الحسابات، الصلاحيات، النسخ الاحتياطي، التحديثات، الاستجابة للحوادث.
HR	ضبط صلاحيات الدخول عند الانضمام/الخروج، تدريب التوعية، إدارة مخالفات السلوك الرقمي.
جميع المستخدمين	الالتزام بكلمات مرور قوية، عدم مشاركة الحسابات، الإبلاغ عن رسائل الاحتيال/الحوادث.

6) تصنيف الأصول والبيانات

- تصنيف البيانات كحد أدنى إلى: (عامة/داخلية/سرية/عالية الحساسية).
- بيانات المستفيدين الصحية/النفسية تُصنف (عالية الحساسية) وتستلزم ضوابط إضافية: تقييد الوصول، تشفير، سجل وصول عند الإمكان.
- يوضع سجل أصول تقنية (DW-REG-IT-ASSET) وسجل حسابات وصلاحيات (DW-REG-IT-ACC).

7) إدارة الهوية والصلاحيات (IAM)

- مبدأ (الحاجة للاطلاع) + (الحد الأدنى من الصلاحيات).
- ممنوع مشاركة الحسابات بين أكثر من شخص.
- MFA إلزامي للبريد/السحابة/الأنظمة الحساسة وحسابات الإدارة.
- إجراءات Onboarding/Offboarding: إنشاء حسابات وصلاحيات وفق طلب معتمد، وإيقافها فور الخروج.
- مراجعة صلاحيات ربع سنوية للحسابات الحساسة ورفع ملخص للجنة الحوكمة/المراجعة.

8) إدارة كلمات المرور والأجهزة

الضابط	المتطلب الأدنى
كلمات المرور	طول ≥ 12 حرف، منع إعادة الاستخدام، تغيير عند الاشتباه.
MFA	إلزامي للحسابات الحساسة/الإدارية.
قفل الشاشة	قفل تلقائي بعد 5–10 دقائق.
تحديثات الأنظمة	تفعيل التحديثات التلقائية أو تحديث شهري على الأقل.
مكافحة البرمجيات الخبيثة	تثبيت برنامج حماية وتحديثه.
تشفير الأجهزة المحمولة	تشفير الهاتف/اللابتوب خصوصاً لمن يحمل بيانات مستفيدين.

9) النسخ الاحتياطي والاستعادة (Backup & Restore)

- نسخ احتياطي دوري (يومي/أسبوعي حسب النظام) مع احتفاظ نسخ لمدة مناسبة.
- تطبيق قاعدة 3-2-1 عند الإمكان: 3 نسخ، 2 وسائط، 1 خارج الموقع/السحابة.
- اختبار استعادة ربع سنوي لعينات وتوثيق النتائج في سجل اختبارات الاستعادة (DW-REG-IT-DRT).
- تقييد الوصول لنسخ الاحتياطي لحسابات محددة فقط.

10) أمن البريد الإلكتروني ومكافحة التصيّد

- تفعيل MFA للبريد الإلكتروني، وتفعيل التنبيهات للولوجات غير المعتادة.
- توعية المستخدمين على رسائل الاحتيال والتصيّد، والاختبار الدوري إن أمكن.
- منع تحويل البريد التلقائي إلى عناوين خارجية دون موافقة مسؤول IT.
- عدم فتح مرفقات مجهولة وعدم مشاركة روابط الدخول أو الرموز.

11) أمن الموردين والأنظمة السحابية

- أي مزود خدمة لديه وصول للبيانات يجب أن يوقع على التزامات سرية وحماية بيانات.
- اشتراط ضوابط أمنية في التعاقدات: MFA، تشفير، سجلات وصول، نسخ احتياطي، إشعار بحوادث.
- تقييم مخاطر المورد قبل منح الوصول للبيانات الحساسة، وربطه بسجل تعارض مصالح الموردين.

12) الاستجابة للحوادث السيبرانية

- الإبلاغ الفوري عند الاشتباه: جهاز مصاب، اختراق بريد، تسريب بيانات، فقد جهاز، رسالة فدية.
- خطة أولية: عزل الجهاز/الحساب، تغيير كلمات المرور، تفعيل التحقيق، إخطار حماية البيانات، توثيق حادث.
- تصنيف الحادث (منخفض/متوسط/عالي) وفق أثره على بيانات المستفيدين والعمليات والسمعة.
- رفع تقرير حادث للمجلس/لجنة المخاطر للحوادث عالية الأثر، مع خطة تصحيح (CAPA).

13) استمرارية الأعمال والتعافي (BCP/DR)

- تحديد الأنظمة الحرجة (بريد/ملفات/CRM/أنظمة مالية) ووضع أولويات استعادة (RTO/RPO) بشكل مبسط.
- توثيق خطة بديلة عند تعطل الأنظمة: قنوات عمل بديلة، نماذج ورقية مؤقتة، وآلية إدخال لاحق.
- اختبار سنوي لخطة الاستعادة أو بعد أي تغيير جوهري.

14) التوعية والتدريب

- تدريب إلزامي سنوي على أمن المعلومات لموظفين ومتطوعين لديهم وصول للأنظمة.
- تدريب خاص لمن يتعامل مع بيانات المستفيدين الحساسة بالتنسيق مع سياسة حماية البيانات.
- توثيق التدريب في سجل التدريب (DW-REG-HR-TRN) وسجل توعية أمنية (DW-REG-IT-AWR).

15) الاستثناءات

- أي استثناء عن ضوابط هذه السياسة يُدار فقط عبر سياسة الاستثناءات (DW-POL-EXC) ويُسجل في سجل الاستثناءات.
- لا يسمح باستثناءات تمس MFA للحسابات الحساسة أو تداول بيانات المستفيدين عبر قنوات غير معتمدة إلا وفق مبرر عالي ومدة محددة وتصعيد.