وقف داركم
سياسة حماية البيانات والخصوصية

رمز الوثيقة: DW-POL-DATA | الإصدار: 1.0

رمز الوثيقة	DW-POL-DATA
الإصدار	1.0
تاريخ الاعتماد	2026/02/05
تاريخ النفاذ	2026/02/15
الجهة المالكة	مجلس الإدارة / لجنة الجودة والحوكمة / الإدارة التنفيذية (COO)
مستوى السرية	داخلي - بيانات حساسة

تهدف هذه السياسة إلى حماية بيانات المستفيدين والمتطوعين والموظفين والشركاء والموردين وجميع أصحاب العلاقة، خصوصًا البيانات الحساسة المتعلقة بالصحة النفسية والحالة الاجتماعية، وذلك عبر ضوابط واضحة لإدارة دورة حياة البيانات (جمع/استخدام/حفظ/مشاركة/إتلاف) مع الالتزام بالأنظمة واللوائح المعمول بها في المملكة العربية السعودية وأي تحديثات لاحقة.

1) الغرض والنطاق

- تنطبق هذه السياسة على جميع البيانات التي يجمعها أو يعالجها أو يحتفظ بها وقف داركم بأي شكل (ورقي/إلكتروني/صور/صوت/فيديو).
- تشمل البيانات: بيانات المستفيدين (الحالات)، بيانات الموظفين والمتطوعين، بيانات المتبرعين عند توفرها، بيانات الموردين والشركاء.
- تغطي السياسة: الخصوصية، السرية، حقوق أصحاب البيانات، مشاركة البيانات مع أطراف ثالثة، أمن المعلومات، الإبلاغ عن الحوادث، والحفظ والإتلاف.
- تُقرأ هذه السياسة مع: سياسة تعارض المصالح، سياسة الصرف، سياسة المشتريات والتعاقدات، سياسة إدارة المخاطر، وسياسة المراجعة الداخلية.

2) تعريفات مختصرة

- البيانات الشخصية: كل بيان يحدد هوية شخص أو يمكن أن يؤدي لتحديدها بشكل مباشر أو غير مباشر.
- البيانات الحساسة: بيانات تتعلق بالصحة (الجسدية/النفسية)، البيانات الطبية، بيانات القاصرين، البيانات المالية للفرد، أو أي بيانات يُحتمل أن يسبب كشفها ضرراً بالغاً.
- صاحب البيانات: الشخص الذي تتعلق به البيانات (مستفيد/موظف/متطوع/متبرع... إلخ).
- المعالجة: أي عملية على البيانات (جمع/تسجيل/حفظ/تعديل/مشاركة/نقل/إتلاف).
- الترميز/إخفاء الهوية: استخدام رمز حالة بدل الاسم لتقليل قابلية التعرف على الشخص.

3) المبادئ الحاكمة لحماية البيانات

- المشروعية والشفافية: جمع ومعالجة البيانات لغرض مشروع وبشكل واضح لصاحب البيانات.
- تحديد الغرض: استخدام البيانات فقط للأغراض المحددة وقت الجمع أو ما يتوافق معها.
- تقليل البيانات: جمع الحد الأدنى اللازم لتحقيق الغرض (Need-to-know).
- الدقة: تحديث البيانات وتصحيح الأخطاء عند اكتشافها.
- تقليل مدة الاحتفاظ: عدم الاحتفاظ بالبيانات أكثر من الحاجة النظامية/التشغيلية.
- السرية والأمن: حماية البيانات من الوصول غير المصرح أو الفقد أو التعديل غير المشروع.
- المساءلة: توثيق القرارات والإجراءات وإثبات الالتزام (Evidence for Governance).

4) تصنيف البيانات ومستويات السرية

التصنيف	أمثلة	مستوى الحماية المطلوب
عامة	معلومات منشورة على الموقع/التقارير العامة	متاح للجمهور بعد مراجعة واعتماد
داخلية	مراسلات داخلية/نماذج تشغيلية غير حساسة	مقيدة داخل الوقف بصلاحيات
سرية	بيانات موردين/عقود/مراسلات مالية	صلاحيات مقيدة + حفظ آمن
سرية جداً (حساسة)	بيانات حالات نفسية/طبية/سكن/صور المستفيدين/بيانات قاصرين	أعلى قيود: أقل عدد وصول + ترميز + تشفير + سجل دخول

5) الحوكمة والأدوار والمسؤوليات

الدور	المسؤوليات
مجلس الإدارة	اعتماد السياسة ومراقبة الالتزام وتلقي التقارير الجوهرية والحوادث الجسيمة.
لجنة الجودة والحوكمة	تحديث سجل السياسات، متابعة الالتزام، رفع تقارير دورية وتحسينات.
COO / الإدارة التنفيذية	تطبيق الضوابط، تعيين مسؤول حماية بيانات (إن وجد)، إدارة الحوادث، ضمان تدريب العاملين.
مسؤول حماية البيانات (DPO/منسق)	إدارة برنامج الخصوصية، استقبال طلبات أصحاب البيانات، مراجعة مشاركة البيانات والعقود، متابعة الامتثال والتوعية.
مالكو البيانات (مدراء البرامج/الحالات)	التأكد من جمع البيانات بشكل صحيح وبحدود الحاجة، وحفظها وفق الضوابط، والإبلاغ عن أي حادث.
تقنية المعلومات/الأمن السيبراني (إن وجد)	تطبيق الضوابط التقنية: صلاحيات، نسخ احتياطي، تشفير، سجلات دخول، حماية الأجهزة.
الموظفون/المتطوعون	الالتزام بالسرية، استخدام البيانات للأغراض المصرح بها فقط، عدم مشاركة البيانات عبر قنوات غير معتمدة.
الأطراف الثالثة (مزودون/شركاء)	الالتزام ببنود حماية البيانات في العقد، وعدم استخدام البيانات إلا وفق تعليمات الوقف.

6) الأساس النظامي/الموافقة وإشعارات الخصوصية

- يجمع الوقف بيانات المستفيدين لتحقيق أهداف الوقف (تقديم الرعاية/الإحالة/الدعم) مع الالتزام بشرط الواقف ومصارف الوقف.
- عند الحاجة، تُستحصل موافقة صريحة ومستنيرة من صاحب البيانات أو وليه/وصيه خصوصًا للبيانات الحساسة أو مشاركة البيانات مع طرف ثالث.
- يوضح إشعار الخصوصية: نوع البيانات، الغرض، الجهات التي قد تُشارك معها البيانات، مدة الاحتفاظ، وحقوق صاحب البيانات وآلية التواصل.
- للتصوير/النشر الإعلامي: يلزم نموذج موافقة منفصل (Photo/Media Consent) مع حق الرفض دون تأثير على الخدمة.

7) جمع البيانات وتقليلها وترميز الحالات

- يتم جمع الحد الأدنى من البيانات اللازمة لتقديم الخدمة أو إثبات الاستحقاق أو الامتثال.
- تستخدم رموز الحالات (Case ID) بدل الأسماء في المذكرات والتقارير الداخلية قدر الإمكان.
- تُمنع مشاركة ملفات الحالات الحساسة عبر تطبيقات غير معتمدة أو مجموعات عامة (واتساب/تلغرام... إلخ).
- عند مشاركة بيانات لأغراض إحالة علاجية/اجتماعية، تُشارك البيانات الضرورية فقط وبقنوات آمنة ومعتمدة.

8) ضوابط الوصول والصلاحيات (Need-to-know)

- تُحدد الصلاحيات بناءً على الدور الوظيفي (Role-Based Access) وتراجع دوريًا (ربع سنوي على الأقل) أو عند انتقال الموظف/المتطوع.
- يمنع استخدام حسابات مشتركة، وتستخدم كلمات مرور قوية ومصادقة متعددة العوامل (MFA) إن أمكن.
- تُسجل عمليات الدخول على الأنظمة الحساسة وتراجع عند الحاجة (Logs).
- يُلغى الوصول فور انتهاء العلاقة الوظيفية أو التطوعية.

9) أمن البيانات (ضوابط تقنية وتشغيلية)

- التشفير: تشفير الأجهزة المحمولة والملفات الحساسة عند التخزين/الإرسال إن أمكن.
- النسخ الاحتياطي: نسخ احتياطي دوري للبيانات الحيوية مع اختبار الاستعادة.
- الحماية من البرمجيات الخبيثة: تحديثات أمنية، مكافح فيروسات، وتقييد تثبيت البرامج.
- الأمن المادي: حفظ الملفات الورقية في خزائن مقفلة، وتقييد الوصول لغرف الأرشيف.
- العمل عن بعد: استخدام قنوات معتمدة، وتجنب حفظ بيانات حساسة على أجهزة شخصية دون ضوابط.
- إخفاء الهوية عند التحليل: استخدام بيانات مجمعة/مجهولة عند إعداد تقارير أثر/إحصاءات.

10) مشاركة البيانات والأطراف الثالثة

- لا تُشارك البيانات مع أي طرف ثالث إلا لغرض مشروع ومحدد (تقديم خدمة/إحالة/امتثال/تعاقد) وبالحد الأدنى اللازم.
- تُوثق مشاركة البيانات في (سجل مشاركة البيانات) ويشمل: الجهة، الغرض، نوع البيانات، التاريخ، أساس المشاركة، قناة الإرسال.
- يجب تضمين بنود حماية البيانات في عقود الموردين/الشركاء (Data Processing Clauses) وتحديد مسؤوليات الطرف الثالث.
- أي مشاركة مع جهات تنظيمية/أمنية تتم وفق الأنظمة ذات العلاقة وبالتنسيق مع الإدارة العليا.

11) نقل البيانات خارج المملكة/الخدمات السحابية

- يُفضل استضافة البيانات الحساسة داخل المملكة أو لدى مزود يحقق متطلبات الأمن والخصوصية.
- عند الحاجة لاستخدام خدمات سحابية/نقل بيانات خارج المملكة، يلزم تقييم مسبق للمخاطر وموافقة الإدارة العليا وفق التفويض، وتوثيق الضمانات التعاقدية.

12) الاحتفاظ بالبيانات والإتلاف الآمن

- تحدد مدة الاحتفاظ وفق المتطلبات النظامية والتشغيلية وبما يحقق الغرض، وتوثق في (جدول الاحتفاظ والإتلاف).
- بعد انتهاء مدة الاحتفاظ، تُتلف البيانات بشكل آمن: تمزيق/إتلاف ورقي، ومسح آمن/إزالة نهائية للملفات الإلكترونية.
- يحظر الاحتفاظ بنسخ شخصية غير معتمدة من ملفات المستفيدين أو إرسالها للبريد الشخصي.

13) حقوق أصحاب البيانات وآلية التعامل مع الطلبات

- يحق لصاحب البيانات – ضمن الحدود النظامية – طلب: الاطلاع، الحصول على نسخة، التصحيح، الإتلاف/الحذف (عند انقضاء الغرض)، أو سحب الموافقة (إن كانت الأساس).
- تُستقبل الطلبات عبر قناة رسمية (بريد/نموذج) وتوثق في (سجل طلبات أصحاب البيانات) مع التحقق من الهوية قبل الاستجابة.
- تُحدد مدد الاستجابة وإجراءاتها داخليًا بما يضمن عدم الإضرار بحقوق الأطراف أو الالتزامات النظامية.

14) إدارة حوادث تسرب/اختراق البيانات (Data Breach)

- أي موظف/متطوع يشتبه بحادث (فقد جهاز/إرسال خاطئ/اختراق) يبلغ فورًا الإدارة التنفيذية/مسؤول حماية البيانات.
- يتم تصنيف الحادث (منخفض/متوسط/عالٍ/جسيم) حسب نوع البيانات وعدد المتأثرين وخطورة الأثر.
- إجراءات الاستجابة: احتواء الحادث ← تقييم الأثر ← معالجة السبب ← توثيق كامل ← إجراءات تصحيحية (CAPA).
- عند الحوادث الجسيمة، يتم إشعار مجلس الإدارة، واتخاذ ما يلزم لإشعار المتأثرين/الجهات المختصة وفق المتطلبات النظامية.

15) التدريب والتوعية والمراجعة

- تدريب إلزامي سنوي على السرية وحماية بيانات المستفيدين (خصوصًا العاملين على الحالات).
- توقيع تعهدات السرية (NDA) للموظفين والمتطوعين ومن لديهم وصول للبيانات الحساسة.

- مراجعة امتثال دورية عبر لجنة المراجعة الداخلية والتقييم (عينات) ورفع نتائج التحسين للجنة الجودة والحوكمة.

16) المخالفات والجزاءات

- يعد مخالفة جسيمة: مشاركة بيانات حساسة دون صلاحية/موافقة، استخدام قنوات غير آمنة، تصوير/نشر دون موافقة، أو الاحتفاظ بنسخ خارجية غير مصرح بها.
- تطبق الإجراءات التأديبية وفق سياسة الموارد البشرية/السلوك المهني، وقد تصل لإنهاء العلاقة وإحالة الأمر وفق الأنظمة عند اللزوم.

17) المراجعة والتحديث

- تراجع هذه السياسة سنويًا أو عند حدوث تغيير جوهري (أنظمة/أنظمة تشغيل/نطاق خدمات/مزود سحابي).
- يعتمد أي تعديل من مجلس الإدارة، وتوثق النسخ في سجل السياسات.