القسم الأول: السياسات والاجراءات الخاصة بالمستفيدين

الفصل الرابع

سياسات وإجراءات صلاحيات الوصول وحماية وثائق وبيانات المستفيدين

القسم الأول: السياسات والاجراءات الخاصة بالمستفيدين

• الفصل الرابع: سياسة صلاحيات الوصول إلى بيانات المستفيدين

• أولاً: الغرض من السياسة:

- تهدف هذه السياسة إلى تحديد ضوابط وصلاحيات الوصول إلى بيانات المستفيدين، سواء كانت بيانات شخصية أو طبية أو اجتماعية أو مالية، وذلك لضمان سرية المعلومات وحماية خصوصية المستفيدين. تنطبق هذه السياسة على جميع الموظفين والمتعاونين والجهات ذات العلاقة، وتشمل البيانات المخزنة ورقيًا أو إلكترونيًا، بما يتوافق مع الأنظمة والتشريعات المعمول بها.

• ثانيا: صلاحيات الوصول إلى بيانات المستفيدين

م	المسؤول	نوع البيانات المسموح الوصول إليها	مستوى الصلاحية	الهدف من الوصول
.1	الأخصائي الاجتماعي / فريق البحث الاجتماعي وفريق البرامج	• جميع بيانات المستفيدين (الشخصية – الاجتماعية – الطبية – المالية – سجل الخدمات – التقارير – الكشوفات - كافة الملفات والنماذج التشغيلية والمالية للبرنامج)	• وصول كامل	• الاطلاع ومعالجة بيانات المستفيدين الأساسية • تحديث الملفات • مراجعة الوثائق • إدخال البيانات في النظام. • إعداد الدراسات والتقارير • تقديم الخدمات وتنفيذ البرامج
.2	مدير الفرع / الممثلين			• متابعة الأداء اتخاذ القرارات • إدارة الطلبات • الاعتماد النهائي لكافة مخرجات الفرع والممثلين
.3	مشرفة العمل الاجتماعي واخصائية إدارة العمليات	• جميع بيانات المستفيدين (الشخصية – الاجتماعية – الطبية – المالية – سجل الخدمات – التقارير)	• وصول إشرافي	• مراجعة قواعد المستفيدين • مراجعة واعتماد الدراسات • متابعة جودة العمل
.4	مدراء المشاريع والبرامج	• بيانات المستفيدين المرتبطين بالبرنامج فقط • بيانات الحضور والمشاركة • كافة الملفات والنماذج التشغيلية والمالية للبرنامج	• وصول محدود حسب البرنامج	• الاشراف على تنفيذ البرامج • متابعة مؤشرات الأداء والخطط التشغيلية • متابعة جودة العمل

م	المسؤول	نوع البيانات المسموح الوصول إليها	مستوى الصلاحية	الهدف من الوصول
.5	**الإدارة المالية**	• بيانات الدعم المالي فقط • مستندات الصرف والإيصالات • بيانات المستفيد المالية • إقرارات الاستلام	• وصول مقيد	• الصرف • المراجعة • التدقيق المالي
.6	**رئيس العمليات**	• جميع بيانات الفروع والبرامج • تقارير الأداء والنتائج	• وصول إشرافي عالي المستوى	• الاطلاع على بيانات المستفيدين لأغراض تشغيلية وتطويرية، • متابعة التزام الفروع بالسياسات والإجراءات. • اتخاذ قرارات تشغيلية شاملة
.7	**الأمين العام**	• جميع البيانات عند الحاجة (مجمعة أو فردية) + تقارير الأداء والنتائج • تقارير الأداء والنتائج	• وصول استثنائي	• اتخاذ القرارات الاستراتيجية، والاطلاع على التقارير الشاملة لجميع الفروع.
.8	**موظف تقنية المعلومات**	• صلاحيات النظام – إدارة الحسابات – سجلات الدخول – النسخ الاحتياطي	• وصول تقني غير تشغيلي	• حماية البيانات وصيانتها • إدارة النسخ الاحتياطية
.9	**المتعاونون الخارجيون (مزودي خدمة / جهات تقييم / متطوعين)**	• بيانات محددة يتم تحديدها مسبقاً حسب المهمة	• وصول مؤقت محدود	• تنفيذ المهام المحددة، • التقييم والدعم
.10	**الجهات الحكومية والرقابية**	• بيانات يتم تحديدها وفق الطلب الرسمي	• وصول نظامي عند الطلب	• مراقبة الالتزام • التحقق من سلامة الإجراءات

- **ثالثاً: ضوابط الوصول إلى البيانات وآليات التحقق من الهوية وإدارة الصلاحيات:**

1. تطبيق مبدأ "الحد الأدنى من الوصول "بحيث لا يُسمح بالاطلاع إلا على البيانات اللازمة لتنفيذ المهام.
2. إجراء مراجعة دورية لقوائم المستخدمين للتأكد من توافق الصلاحيات مع المهام الفعلية.
3. إلغاء صلاحيات الوصول فورًا عند انتهاء علاقة الموظف بالجهة أو انتقاله لوظيفة لا تتطلب الوصول للبيانات.

- **رابعاً: إجراءات حماية وتخزين الوثائق والبيانات والمعلومات:**

م	الإجراء / نوع الحماية	وصف الإجراء	المسؤول عن التنفيذ
أولاً: حماية الوصول الرقمي			
.1	**كلمات المروروحماية الدخول**	• استخدام كلمات مرور قوية وتغييرها بشكل دوري	• مسؤول تقنية المعلومات • مسؤول الموارد البشرية • جميع الموظفين
.2	**مر اقبة محاولات الاختراق**	• تفعيل تنبيهات تلقائية عند أي محاولة دخول غير مصرح به أو أي محاولات اختراق	
.3	**حماية البيانات الحساسة**	• منع تخزين البيانات على أجهزة غير محمية أو شبكات غير آمنة أو شخصية	
.4	**تسجيل كل عمليات الوصول**	• تفعيل أنظمة تسجيل الدخول والخروج لمراقبة جميع عمليات الوصول	
.5	**مراجعة السجلات الدورية**	• مراجعة النشاط الإلكتروني بشكل دوري للتأكد من عدم وجود أي أنشطة مشبوهة أو غير معتادة	
.6	**حماية الخصوصية**	• منع مشاركة بيانات المستفيدين خارج الجهات المخولة	
ثانياً: النسخ الاحتياطي واستعادة البيانات			
.7	**النسخ الاحتياطي الدوري**	• إنشاء نسخ احتياطية للبيانات والملفات الخاصة بالمستفيدين والانتفاع من الخدمات و الملفات الإدارية والتشغيلية المهمة بشكل دوري وحفظها الاحتياطية في مواقع آمنة ومحمية ضد التلف	• مدراء الفروع • موظفي الفروع • مدراء المشاريع • مشرفة العمل الاجتماعي • اخصائية إدارة العمليات
ثالثاً: حماية الأجهزة والشبكات			
.8	**الحماية من الفيروسات**	• تشغيل برامج الحماية من البرمجيات الضارة وتحديثها بانتظام	• مسؤول تقنية المعلومات • جميع الموظفين
.9	**تحديث الأنظمة**	• تحديث أنظمة التشغيل والتطبيقات بشكل مستمر	
رابعاً: حماية الوصول الورقي			
.10	**حفظ الملفات الورقية**	• حفظ الملفات في أماكن مغلقة وآمنة لا يصل إليها إلا المخولون	• مدراء الفروع • موظفي الفروع • مدراء المشاريع • مشرفة العمل الاجتماعي • اخصائية إدارة العمليات
.11	**منع ترك الوثائق الحساسة**	• عدم ترك أي وثائق في أماكن عامة أو غير مؤمنة	
.12	**التخلص الآمن من المستندات**	• إتلاف المستندات غير الضرورية وفق آلية الإتلاف المعتمدة	

م	الإجراء / نوع الحماية	وصف الإجراء	المسؤول عن التنفيذ
خامساً: الحماية أثناء النقل والمشاركة			
.13	**مشاركة الوثائق بشكل آمن**	• عدم إرسال البيانات إلا عبر قنوات معتمدة ومشفرة	• جميع الموظفين
.14	**إجراءات نقل الملفات الورقية**	• نقل الوثائق بين الفروع أو الجهات بطريقة آمنة وموثقه	

- **خامساً: جدول إجراءات التعامل مع الخرق الأمني وفقدان الوثائق والعقوبات**

م	نوع الحالة	الإجراء	المسؤول	المخرجات المطلوبة
.1	**خرق أمني / محاولة وصول غير مصرح به**	• الإبلاغ الفوري عن الحادث للإدارة المختصة • عزل النظام أو الملف المتضرر لمنع المزيد من الاختراقات • مراجعة سجلات الوصول لتحديد مصدر الخرق • إعادة تعيين كلمات المرور وإصلاح أي ثغرات • إبلاغ الجهات المختصة واتخاذ الإجراءات القانونية	• الموظف المكتشف للخرق • فريق تقنية المعلومات • فريق تقنية المعلومات / الإدارة المختصة • الإدارة العليا / الشؤون القانونية	• تسجيل الحادث رسميًا • حماية البيانات المتضررة • تقرير تحليل الخرق • استعادة أمان النظام • اتخاذ الإجراءات القانونية اللازمة
.2	**فقدان أو تلف وثائق أو ممتلكات**	• إبلاغ الإدارة المختصة فورًا مع توضيح التفاصيل • التحقق من كاميرات المراقبة (إن وجدت) لتحديد السبب • البحث عن حلول لتعويض المستفيد إن كان ذلك ممكنًا. • اتخاذ الإجراءات القانونية في حال الاشتباه بالسرقة أو فقدان مقصود	• الموظف المكتشف • فريق الأمن / الإدارة المختصة • الإدارة المختصة • الشؤون القانونية / الإدارة العليا	• توثيق الحادث رسميًا • تقرير حول سبب الفقدان أو التلف • استكمال حقوق المستفيد إن أمكن • متابعة قانونية رسمية
.3	**انتهاك سياسة البيانات**	• توجيه إنذار رسمي • تعليق أو إلغاء صلاحيات الوصول • اتخاذ إجراءات قانونية بحق المخالف	• الإدارة المختصة / الموارد البشرية • الإدارة العليا / الشؤون القانونية	• إخطار الموظف رسميًا • تقييد الوصول فورًا • متابعة قانونية وإجراءات نظامية

لقد اطلع مجلس إدارة جمعية أسر التوحد الخيرية في اجتماعه رقم (1) بتاريخ 30 مارس 2026م على كافة اللوائح والسياسات والإجراءات بالجمعية، وقرر اعتمادها وتعميمها والعمل بموجبها، ونشرها على الموقع الإلكتروني للجمعية (جمعية أسر التوحد - الرئيسية) (saf.org.sa).

