# جمعية القطيف الخيرية

Qatif Charity Association

# دليل الإجراءات والسياسات

## قسم تقنية المعلومات

| | |
|---|---|
| **رقم الإصدار** | 1.0 |
| **تاريخ الإصدار** | 2026 |
| **جهة الإعداد** | قسم تقنية المعلومات |
| **مستوى السرية** | سري — للاستخدام الداخلي |
| **دورة المراجعة** | سنوية أو عند التغيير التنظيمي |
| **جهة الاعتماد** | مجلس الإدارة |
| **تاريخ الاعتماد** | _____ |

# فهرس المحتويات

**المستوى الأول: السياسات الأمنية والسيادية — فائق الحساسية**

تتعلق سياسات هذا المستوى بحماية سمعة الجمعية وبيانات المتبرعين والمستفيدين. جميع السياسات إلزامية ولا يجوز الاستثناء منها إلا بقرار مكتوب من المدير التنفيذي.

# القسم الأول: سياسة إدارة الوصول والهوية

## 1.1 المصادقة متعددة العوامل (MFA)

**المصادقة متعددة العوامل إلزامية فورياً للفئات التالية:**

- جميع مديري الأنظمة (Admins) — تطبيق فوري
- الموظفون الذين يصلون للأنظمة الحساسة (رافد، Microsoft 365)
- جميع الموظفين عند الوصول عن بُعد (VPN)

**لا يُسمح لأي مدير نظام بتعطيل MFA تحت أي ظرف**

## 1.2 مبدأ أقل الامتيازات

لا يملك أي موظف صلاحيات إدارية دائمة — تمنح عند الحاجة وتُسحب فور انتهاء المهمة.

| الفئة | مستوى الصلاحية | آلية المنح | مدة الصلاحية |
|---|---|---|---|
| مدير النظام | Admin كامل | قرار مجلس الإدارة | دائمة مع مراجعة سنوية |
| مدير تقنية | Admin محدود | قرار المدير التنفيذي | دائمة مع مراجعة ربع سنوية |
| فني تقنية | User مرتفع | طلب صلاحية موثق | حسب المهمة |
| موظف عادي | User عادي | طلب صلاحية موثق | حسب المنصب |
| صلاحية مؤقتة | Admin مقيّد | تذكرة + موافقة مديرين | 48 ساعة كحد أقصى |

## 1.3 الفصل بين المهام في نظام رافد

يُحظر جمع الصلاحيتين التاليتين لدى شخص واحد في نظام رافد:

- صلاحية إدخال بيانات التبرعات
- صلاحية إدارة قاعدة البيانات والتقارير المالية

# القسم الثاني: سياسة أمن البريد الإلكتروني

## 2.1 حماية نطاق الجمعية

- تطبيق بروتوكولات SPF وDKIM وDMARC لمنع انتحال اسم الجمعية
- مراجعة دورية لسجلات DNS كل 6 أشهر
- الإبلاغ الفوري عن أي محاولة انتحال

## 2.2 خصوصية بريد الموظفين

| | |
|---|---|
| **الشرط المطلوب** | إذن مكتوب من المدير التنفيذي |
| **الغرض المسموح به** | أغراض التحقيق فقط |
| **التوثيق المطلوب** | توثيق التاريخ والسبب والشخص المنفذ |
| **الاحتفاظ بالسجل** | أرشفة الإذن لمدة سنتين على الأقل |

## 2.3 مكافحة التصيد الاحتيالي

- تدريب ربع سنوي لجميع الموظفين
- تجارب تصيد دورية لقياس اليقظة
- الإبلاغ الفوري عن أي بريد مشبوه

# القسم الثالث: سياسة نظام المراقبة (الكاميرات)

## 3.1 إدارة كلمات المرور

| | |
|---|---|
| **حفظ كلمات المرور** | ظرف مختوم داخل خزنة الجمعية لدى المدير التنفيذي |
| **دورة التغيير** | كل 6 أشهر أو عند تغيير الموظف المسؤول |
| **التوثيق** | تسجيل تاريخ كل تغيير في سجل رسمي |

## 3.2 إجراءات سحب التسجيلات

نموذج طلب الاطلاع يجب أن يتضمن:

- اسم الطالب وصفته الوظيفية
- سبب الطلب بالتفصيل
- التاريخ والوقت المطلوب
- اسم الشخص الذي قام بالاستخراج
- توقيع المدير التنفيذي للموافقة

**يُحصر الوصول لعملية استخراج المقاطع على شخصين فقط معتمدين من المدير التنفيذي**

المستوى الثاني: حوكمة الأصول والمشتريات — عالي الأهمية

# القسم الرابع: سياسة المشتريات التقنية

## 4.1 متطلبات دراسة الجدوى

لا يُعتمد أي مشروع تقني أو شراء إلا بدراسة جدوى موثقة تشمل:

- التكلفة الإجمالية (شراء + صيانة + تشغيل)
- العائد المتوقع وأثره على الكفاءة التشغيلية
- فترة الاسترداد المتوقعة
- مخاطر التشغيل والبدائل المتاحة
- مقارنة بين 3 موردين على الأقل

## 4.2 آلية المشتريات

| الدور | الجهة |
|---|---|
| يحدد المواصفات الفنية (جهة التوصية) | قسم تقنية المعلومات |
| تختار بين الموردين بشكل مستقل | لجنة المشتريات |
| تنفذ العقد (جهة الترسية) | الإدارة المالية |
| يوقعان نموذج استلام | تقنية + المستخدم |

## 4.3 مستلزمات الموظف القياسية

| الجهاز | المواصفات الدنيا | دورة التجديد |
|---|---|---|
| حاسب مكتبي أو محمول | Intel i5 / 8GB RAM / 256GB SSD | 5 سنوات |
| شاشة | Full HD / 24 بوصة | 7 سنوات |
| هاتف Grandstream | IP Phone معتمد | 5 سنوات |
| طابعة شبكية | مشتركة بين الأقسام | لا تُخصص فردية |

# القسم الخامس: سجل الأصول الرقمي (Snipe-IT)

## 5.1 الجرد والتوثيق

- جرد فوري لجميع الأجهزة وربطها بنظام Snipe-IT
- تحديد الموقع والمسؤول لكل جهاز
- نموذج استلام إلزامي عند تسليم أي جهاز للموظف
- مسح البيانات بشكل آمن قبل التخلص من أي جهاز

## 5.2 سياسة الإهلاك والإتلاف

| | |
|---|---|
| **معيار الإهلاك** | انتهاء دورة التجديد أو التلف الكلي الموثق |
| **مسح البيانات** | استخدام برنامج مسح معتمد + توثيق العملية |
| **التخلص من الجهاز** | بيع / تبرع / إتلاف — بقرار لجنة مشتريات |
| **التوثيق** | نموذج إهلاك معتمد من إدارة الأصول |

## المستوى الثالث: العمليات التشغيلية — مهم لاستمرارية العمل

# القسم السادس: إجراءات دورة حياة الموظف

## 6.1 استقبال موظف جديد — Onboarding

**يجب استلام طلب الاستقبال من HR قبل 48 ساعة من بدء الموظف**

| | |
|---|---|
| 1 | HR ترفع تذكرة Onboarding: الاسم، المنصب، القسم، تاريخ البدء |
| 2 | إنشاء حساب Active Directory + تعيين كلمة مرور مؤقتة |
| 3 | إنشاء بريد Microsoft 365 مرتبط بالـ AD |
| 4 | تهيئة جهاز الحاسب (Windows + برامج القسم + Bitdefender) |
| 5 | إنشاء تحويلة هاتفية في نظام Grandstream |
| 6 | منح صلاحيات الأنظمة حسب المنصب (رافد، طابعة، Canva) |
| 7 | إضافة البريد لقوائم التوزيع المناسبة |
| 8 | تسليم الجهاز بنموذج عهدة + تسجيل في Snipe-IT |
| 9 | جلسة توجيه تقني للموظف (30 دقيقة) |
| 10 | إغلاق التذكرة وإشعار HR بالإتمام |

## 6.2 مغادرة موظف / متطوع / متدرب — Offboarding

**يجب إشعار قسم تقنية المعلومات قبل 72 ساعة من آخر يوم عمل**

| | |
|---|---|
| 1 | HR ترفع تذكرة Offboarding: الاسم، آخر يوم عمل، سبب الإنهاء |
| 2 | نسخ احتياطي فوري للبريد الإلكتروني والبيانات المهنية |
| 3 | ضبط الرد التلقائي وتحويل البريد للمدير المباشر |
| 4 | تعطيل حساب Active Directory في آخر يوم عمل |
| 5 | إلغاء جميع الصلاحيات: رافد، Canva، VPN، Microsoft 365 |
| 6 | إلغاء التحويلة الهاتفية في Grandstream |
| 7 | حذف وصول Bitdefender من الأجهزة الشخصية إن وجدت |
| 8 | استرداد جميع الأجهزة وتوثيق في Snipe-IT |
| 9 | إزالة البريد من قوائم التوزيع |
| 10 | إغلاق التذكرة + نموذج تسليم موقع + إشعار HR |

### 6.3 نقل موظف بين الأقسام

| | |
|---|---|
| 1 | HR ترفع تذكرة نقل قبل 48 ساعة من تاريخ النقل |
| 2 | تحديث بيانات الموظف في Active Directory والـ Microsoft 365 |
| 3 | مراجعة وتعديل صلاحيات الأنظمة حسب المنصب الجديد |
| 4 | إلغاء صلاحيات المنصب السابق فور التنفيذ |
| 5 | تحديث قوائم التوزيع البريدية |
| 6 | تحديث سجل Snipe-IT بالموقع الجديد |
| 7 | إغلاق التذكرة وإشعار المديرين المعنيين |

## القسم السابع: إجراءات الدعم الفني وفتح التذاكر

### 7.1 قنوات تقديم الدعم

يُقدَّم طلب الدعم عبر نظام التذاكر الإلكتروني حصراً — لا يُقبل طلب غير موثق.

**الرابط: https://erp.qatifcharity.org/it_helpdesk**

### 7.2 مستويات SLA

| التصعيد | وقت الحل | أول رد | الأولوية |
|---|---|---|---|
| 2 ساعة | 4 ساعات | 1 ساعة | حرج |
| 6 ساعات | 8 ساعات | 4 ساعات | عالٍ |
| 20 ساعة | 24 ساعة | 8 ساعات | متوسط |
| 48 ساعة | 72 ساعة | 24 ساعة | منخفض |

### 7.3 فئات الطلبات وإجراءات كل فئة

#### أ. استقبال موظف جديد / إنهاء خدمات

- HR ترفع التذكرة قبل 48 / 72 ساعة على التوالي
- يُرفق قرار التعيين أو إنهاء الخدمة الرسمي
- SLA: تنفيذ كامل في اليوم الأول / الأخير

#### ب. طلب صيانة جهاز

- يُوضح نوع العطل بالتفصيل ومتى بدأ
- يُرفق صورة للخطأ إن أمكن
- SLA حسب الأولوية (حرج: 4 ساعات / عادي: 24 ساعة)

#### ج. طلب تثبيت برنامج

- لا يُثبَّت أي برنامج دون تذكرة معتمدة

- فحص البرنامج بـ Bitdefender قبل التثبيت
- البرامج المدفوعة تستلزم دراسة جدوى وموافقة إدارية

### د. طلب صلاحية نظام (رافد أو غيره)

- يمر بمسار الموافقة: مدير مباشر ← مدير تقنية
- توضيح المبرر الوظيفي
- SLA: تنفيذ خلال 4 ساعات من اعتماد الصلاحية

### هـ. نسيت كلمة المرور / اسم المستخدم

| | |
|---|---|
| 1 | الموظف يرفع تذكرة أو يتصل مباشرة بالدعم التقني |
| 2 | التحقق من هوية الموظف (رقم الموظف + سؤال أمني) |
| 3 | إعادة تعيين كلمة مرور مؤقتة وإبلاغ الموظف |
| 4 | إلزام الموظف بتغيير كلمة المرور عند أول دخول |
| 5 | توثيق العملية في سجل التدقيق |

### و. طلب الاطلاع على تسجيلات الكاميرات

| | |
|---|---|
| 1 | تعبئة النموذج الرسمي: السبب، التاريخ، الوقت |
| 2 | تقديم النموذج للمدير التنفيذي للموافقة الخطية |
| 3 | إرسال النموذج المعتمد لقسم تقنية المعلومات |
| 4 | استخراج المقطع من قبل الشخصين المعتمدين فقط |
| 5 | تسليم المقطع وتوثيق العملية كاملاً في السجل |

## القسم الثامن: إدارة الطابعات الشبكية

### 8.1 السياسة العامة

- الاعتماد الكامل على الطابعات الشبكية (Static IP) — يُحظر الطابعات الشخصية
- كل طابعة مشتركة بين قسم أو طابق كامل
- تسجيل جميع الطابعات في نظام Snipe-IT

### 8.2 الصيانة والمتابعة

| | |
|---|---|
| **الصيانة الوقائية** | كل 6 أشهر أو حسب توصية المورد |
| **تتبع الأحبار** | تسجيل الاستهلاك الشهري في سجل رسمي |
| **الطلبات الاستهلاكية** | تذكرة + موافقة المدير قبل الطلب |
| **مسح البيانات** | مسح الذاكرة الداخلية قبل الصيانة الخارجية أو الإهلاك |

## المستوى الرابع: الرقابة الإدارية والتطوير — تنظيمي

# القسم التاسع: الخدمات التقنية المعتمدة

| الخدمة | الوظيفة | آلية الطلب |
|---|---|---|
| Microsoft 365 Admin | إدارة البريد والحسابات المؤسسية | تذكرة Onboarding/Offboarding |
| Active Directory | إدارة هويات المستخدمين | تذكرة + موافقة مدير تقنية |
| Bitdefender GravityZone | الحماية من الفيروسات | تلقائي عند التهيئة |
| Grandstream | نظام الهاتف IP | تذكرة |
| Snipe-IT | إدارة سجل الأصول التقنية | داخلي — يديره قسم التقنية |
| Canva | التصميم الجرافيكي المؤسسي | تذكرة + تحديد الصلاحية |
| Taqnyat | WhatsApp API SMS | طلب إداري + عقد مع المورد |
| نظام رافد | إدارة المستفيدين والمتبرعين | صلاحية مدروسة + فصل مهام |

# القسم العاشر: الاجتماعات الدورية ومؤشرات الأداء

## 10.1 الاجتماعات الدورية

| نوع الاجتماع | الدورية | المشاركون | المخرجات |
|---|---|---|---|
| متابعة مع الأقسام | ربع سنوي | مدير تقنية + ممثلو الأقسام | محضر + قائمة مشكلات |
| مراجعة الأمن السيبراني | نصف سنوي | مدير تقنية + المدير التنفيذي | تقرير مخاطر |
| مراجعة مؤشرات الأداء | شهري | فريق تقنية المعلومات | تقرير SLA وأداء |
| مراجعة السياسات | ???? | تقنية + إدارة + مجلس الإدارة | نسخة محدَّثة معتمدة |

## 10.2 مؤشرات الأداء الرئيسية (KPIs)

| المؤشر | الهدف | آلية القياس |
|---|---|---|
| معدل الالتزام بـ SLA | ≤ 90% | نظام التذاكر شهرياً |
| متوسط وقت حل التذكرة | ≤ 8 ????? | نظام التذاكر |
| الأجهزة الموثقة في Snipe-IT | 100% | مراجعة ربع سنوية |
| MFA ????? | 100% | تقرير Azure AD |
| تدريب التوعية السيبرانية | 100% سنوياً | سجل التدريب |
| مراجعة الصلاحيات | كل 3 أشهر | سجل الصلاحيات |

# القسم الحادى عشر: خطة الاستجابة للحوادث السيبرانية

## 11.1 تصنيف الحوادث

| المستوى | الوصف | وقت الاستجابة |
|---|---|---|
| 🔴 حرج | اختراق بيانات أو توقف كامل للأنظمة | 1 ساعة |
| 🟠 عالي | إصابة بفيروس أو فقدان وصول قسم كامل | 4 [illegible] |
| 🟡 متوسط | محاولة تصيد مكتشفة أو اشتباه أمني | 8 [illegible] |
| 🟢 منخفض | سلوك غير معتاد أو استفسار أمني | 24 ساعة |

## 11.2 إجراءات الاستجابة

| | |
|---|---|
| 1 | الموظف يبلّغ قسم تقنية المعلومات فوراً دون حذف أي شيء |
| 2 | فصل الجهاز أو النظام المتضرر من الشبكة فوراً |
| 3 | تحديد نطاق الحادثة ومصدرها |
| 4 | إشعار المدير التنفيذي خلال 30 دقيقة |
| 5 | تطبيق الإجراءات التصحيحية واحتواء الاختراق |
| 6 | إبلاغ هيئة الأمن السيبراني خلال 72 ساعة عند لزوم |
| 7 | استعادة الأنظمة من النسخ الاحتياطية المعتمدة |
| 8 | تقرير كامل خلال 48 ساعة + الدروس المستفادة |

## 11.3 سياسة النسخ الاحتياطي

| السياسة | العنصر |
|---|---|
| يومي للبيانات الحيوية — أسبوعي للأرشيف | تكرار النسخ |
| AES-256 [illegible] | التشفير |
| 90 يوماً يومية — سنة أسبوعية | مدة الاحتفاظ |
| شهرياً بشكل إلزامي | اختبار الاستعادة |

# الملحق الأول: نماذج العمل الرسمية

## أ. نموذج طلب استخراج تسجيل كاميرا

| | |
|---|---|
| اسم الطالب | _____ |
| الصفة الوظيفية | _____ |
| سبب الطلب | _____ |
| التاريخ المطلوب | _____ |
| الوقت المطلوب | _____ |
| اسم منفذ الاستخراج | _____ |
| توقيع المدير التنفيذي | _____ :□□□□□□□ _____ |

## ب. نموذج عهدة الأصل التقني

| | |
|---|---|
| اسم الموظف | _____ |
| الرقم الوظيفي | _____ |
| نوع الجهاز | _____ |
| الرقم التسلسلي | _____ |
| تاريخ الاستلام | _____ |
| حالة الجهاز | ☐ جديد ☐ مستعمل جيد ☐ مستعمل |
| توقيع الموظف | _____ |
| توقيع مدير تقنية | _____ |

## ج. نموذج تسليم موظف مغادر

| | |
|---|---|
| اسم الموظف | _____ |
| آخر يوم عمل | _____ |
| نسخ احتياطي للبيانات | ☐ □□ □□□□□□□: _____ |
| تعطيل حساب **AD** | ☐ □□ □□□□□□□: _____ |
| إلغاء **Microsoft 365** | ☐ □□ □□□□□□□: _____ |
| إلغاء صلاحيات رافد | ☐ □□ □□□□□□□: _____ |
| إلغاء التحويلة **Grandstream** | ☐ □□ □□□□□□□: _____ |
| استرداد الأجهزة | ☐ □□ □□□□□□□: _____ |
| توقيع الموظف المغادر | _____ |
| توقيع مدير تقنية | _____ |

## الملحق الثانى: سجل مراجعات الوثيقة

| وصف التغيير | المعدِّل | التاريخ | الإصدار |
|---|---|---|---|
| الإصدار الأول | قسم تقنية المعلومات | 2026 | 1.0 |
| | | | |
| | | | |

## الملحق الثالث: توقيعات الاعتماد

| | |
|---|---|
| إعداد | _____ :□□□□□□□ _____ |
| مراجعة — مدير تقنية | _____ :□□□□□□□ _____ |
| اعتماد — المدير التنفيذي | _____ :□□□□□□□ _____ |
| اعتماد — مجلس الإدارة | _____ :□□□□□□□ _____ |

هذا الدليل وثيقة إدارية رسمية معتمدة — يُراجع ويُحدَّث سنوياً أو عند أي تغيير تنظيمي أو تقني جوهري