

## سياسات إدارة التقنية وتكنولوجيا المعلومات

## إدارة التقنية وتكنولوجيا المعلومات

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

# المادة الأولى: سياسة أمن المعلومات

## بطاقة سياسة أمن المعلومات

2025	تاريخ المراجعة	2025/5/1 8	تاريخ التحديث	10/01/202 3	تاريخ الإصدار	1	رقم الإصدار	IT-08- P1	رمز السياسة
------	-------------------	---------------	------------------	----------------	---------------	---	----------------	--------------	----------------

## إدارة التقنية وتكنولوجيا المعلومات

### 1. الأهداف

تهدف هذه السياسة إلى توضيح آليات حماية البيانات في الجمعية ومسؤوليات موظفين إدارة تقنية المعلومات تجاهها، كما توضح مسؤوليات الموظف تجاه أمن المعلومات وصلاحياته وتوفير الحد الأدنى من المتطلبات الأساسية للأمن السيبراني المبنية على أفضل الممارسات والمعايير لتقليل المخاطر السيبرانية على الأصول المعلوماتية والتقنية للجهات من التهديدات (Threats) الداخلية والخارجية. وتتطلب حماية الأصول المعلوماتية والتقنية للجهة التركيز على الأهداف الأساسية للحماية، وهي:

سرية المعلومة Confidentiality

■ سلامة المعلومة Integrity

■ توافر المعلومة Availability

تتبع هذه السياسة متطلبات الهيئة الوطنية للأمن السيبراني التي قامت بتطوير الضوابط الأساسية للأمن السيبراني (ECC – 1: 2018) بعد دراسة معايير وأطر وضوابط للأمن السيبراني قامت بإعدادها سابقاً عدة جهات (محلية ودولية)، ودراسة متطلبات التشريعات والتنظيمات والقرارات الوطنية ذات العلاقة.

### 2. نطاق العمل

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة بالجمعية الفيسالية، وتنطبق على جميع العاملين فيها

### 3. بنود السياسة

#### 1.3 النسخ الاحتياطي

- تحديد البيانات الأكثر أهمية والدرجة وذلك من خلال عملية تصنيف البيانات ومن خلال مراجعة أصول المعلومات، لمنحها أولوية أعلى أثناء عملية النسخ الاحتياطي للشبكة المحلية.
- وضع خطة نسخ احتياطي واستعادة لجميع أصول (البيانات والمعلومات) بالتنسيق بين إدارة التقنية ومع مالك النظام عند الاشتراك في أنظمة سحابية مع الأخذ بالاعتبار التالي:
  - المتطلبات القانونية والتنظيمية.
  - تصنيف الأصول (البيانات والمعلومات).
  - توصيات الموردين
- تحديد النظام المستخدم للنسخ الاحتياطي مع مراعاة البنود التالية في النسخ والاستعادة:
  - نوع النسخ الاحتياطي.
  - جدول النسخ الاحتياطي وتكراره بشكل يومي وأسبوعي.
  - حماية النسخ الاحتياطي (بناء على تصنيف البيانات المنسوخة).
  - الاحتفاظ بالنسخ الاحتياطي.

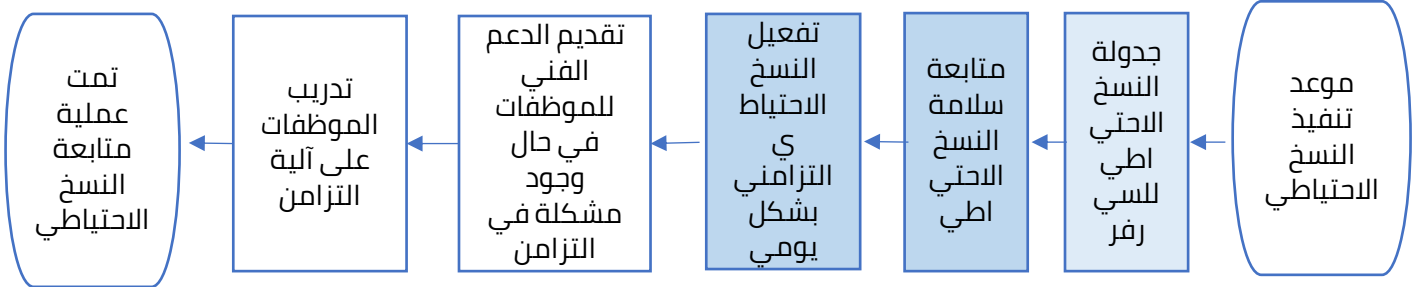
## إدارة التقنية وتكنولوجيا المعلومات

- مراجعة واختبار البيانات المنسوخة احتياطياً بشكل دوري. (كل ثلاثة أشهر) للتأكد من سلامتها وفعاليتها خلال عملية استعادة بيانات محددة
- تفويض الصلاحيات بالتنسيق بين إدارة التقنية ومالك النظام السحابي في عملية تنفيذ واستعادة النسخ الاحتياطية
- منع تعطل مزامنة وحدة التخزين الاحتياطي مع جهاز الموظف.
- يجب استخدام مؤشر قياس الأداء KPI لضمان التطوير المستمر لإدارة حزم التحديثات والإصلاحات.
- مراجعة السياسة وإجراءاتها سنوياً، وتوثيق التغييرات واعتمادها

### عملية النسخ الاحتياطي

هدف العملية	متابعة تنفيذ عملية النسخ الاحتياطي	المسؤول عن تنفيذ العملية	مسؤولية الشبكات
المستهدفون من العملية	قواعد بيانات الجمعية	الوقت اللازم لتنفيذ العملية	أسبوع عمل
مدخلات العملية	الخطوات الإجرائية للعملية	النموذج/ النظام الإلكتروني	مخرجات العملية
جدولة النسخ الاحتياطي	1	البداية: موعد تنفيذ النسخ الاحتياطي	لوحة تحكم نظام النسخ الاحتياطي
	2	جدولة النسخ الاحتياطي للسيرفر المحلي بشكل أسبوعي على سيرفر سحابي ويشمل ملفات الشير وقواعد البيانات	
	3	متابعة سلامة النسخ الاحتياطي على داش بورد	
	4	تفعيل النسخ الاحتياطي التزامني بشكل يومي، وتوفير مساحة TB1 على (ون درايف) لكل موظفة	
	5	تقديم الدعم الفني للموظفات في حال وجود مشكلة في التزامن	
	6	التأكد من وجود المجلدات على D للحد من خسارة المعلومات في حال إعادة تهيئة الجهاز	
	7	تدريب الموظفات على آلية التزامن للتأكد من متابعة الموظفة لملفاتها	
	8	تفعيل برنامج التزامن على جوال الموظفة (في حال رغبها)	
مؤشرات أداء العملية	نسبة تنفيذ عمليات النسخ الأسبوعية واليومية	مخاطر العملية	التأثير على سلامة بيانات الجمعية

## مخطط عملية النسخ الاحتياطي



### 2.3 أمن الشبكة وأجهزة المستخدمين

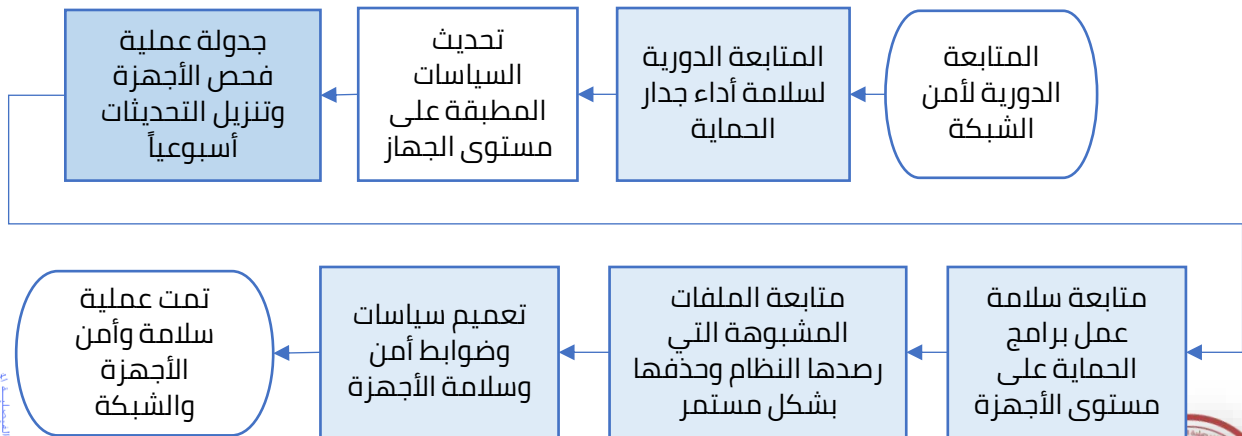
- توفير تقنيات الحماية اللازمة لمكافحة الفيروسات، والبرمجيات الضارة على خوادم الجمعية وأجهزة الحاسب والشبكة.
- إجراء مسح دوري على الأجهزة للكشف عن الثغرات وحزم التحديثات ومتابعة تطبيقها.
- منع تعطيل عمل نظام مكافحة الفيروسات إلا من قبل أخصائي تقنية المعلومات
- معالجة تهديدات البرمجيات الخبيث وأي إصابات بشكل عاجل وفوري وبدون أي تأجيل وبأي شكل كان، وتوثيق ذلك في سجل التهديدات الأمنية.
- إدارة أجهزة المستخدمين والأجهزة المحمولة مركزياً من خلال خادم الدليل النشط Active Directory الخاص بنطاق الجمعية
- تطبيق سياسة مصادقة متعددة العوامل على المستخدمين Multi-Factor Authentication (MFA) لضمان الوصول الآمن إلى الموارد في الجمعية
- تغيير كلمات المرور لحسابات المستخدمين والبريد الإلكتروني كل ثلاثة أشهر.
- ضبط إعدادات أجهزة المستخدمين بإدارة الوحدات التنظيمية المناسبة Domain Controller لتطبيق السياسات الملائمة وتثبيت الإعدادات البرمجية اللازمة
- تنفيذ سياسات النطاق المناسبة Group Policy في الجمعية على جميع الأجهزة لضمان الالتزام بالضوابط التنظيمية والأمنية
- عدم منح العاملين صلاحيات هامة وحساسة على أجهزة المستخدمين ويجب منح الصلاحيات وفقاً لمبدأ الحد الأدنى من الصلاحيات والامتيازات.
- مزامنة التوقيت Clock Synchronization مركزياً ومن مصدر موثوق لجميع أجهزة المستخدمين.
- تنزيل البرامج وحزم التحديثات من مصادر مرخصة وموثوقة على أجهزة المستخدمين والخوادم، بما في ذلك أنظمة التشغيل والبرامج والتطبيقات وفقاً للإجراءات المتبعة داخل الجمعية الفيصلية مره واحدة شهرياً على الأقل.
- السماح فقط بقائمة محددة من المواقع والتطبيقات على أجهزة المستخدمين .
- منع استخدام وسائط التخزين الخارجية، ويجب الحصول على إذن مسبق من إدارة تقنية المعلومات لامتلاك صلاحية استخدامها.

## إدارة التقنية وتكنولوجيا المعلومات

### عملية سلامة وأمن الأجهزة والشبكة الداخلية

مسئولة الشبكات	المسؤول عن تنفيذ العملية	سلامة وأمن الأجهزة والشبكة الداخلية	هدف العملية
أسبوع عمل	الوقت اللازم لتنفيذ العملية	جميع الأجهزة والشبكة الداخلية	المستهدفون من العملية
مخرجات العملية	النموذج/ النظام الإلكتروني	الخطوات الإجرائية للعملية	مدخلات العملية
- تقرير الصيانة	تقرير الصيانة	1 البداية: المتابعة الدورية لأمن الشبكة	جدول - عملية فحص الأجهزة
- تقارير مستوى الحماية على الأجهزة		2 المتابعة الدورية لسلامة أداء جدار الحماية على مستوى السيرفر والشبكة وتحديث السياسات بناء على الاحتياجات الأمنية	
-تقرير بالملفات المشبوهة على الأجهزة		3 تحديث السياسات المطبقة على مستوى الجهاز	
-تقرير بالملفات المشبوهة على الأجهزة		4 جدولة عملية فحص الأجهزة وتنزيل التحديثات أسبوعياً، وإرسال رسالة التذكير بترك الأجهزة مفتوحة بعد الدوام	
-تقرير بالملفات المشبوهة على الأجهزة		5 متابعة سلامة عمل برامج الحماية على مستوى الأجهزة وتحديث قاعدة البيانات الخاصة بالقسم عن حالة الجهاز	
-تقرير بالملفات المشبوهة على الأجهزة		6 متابعة الملفات المشبوهة التي رصدها النظام وحذفها بشكل مستمر	
-تقرير بالملفات المشبوهة على الأجهزة		7 تعميم سياسات وضوابط أمن وسلامة الأجهزة وملحقاتها	
التأثير على أعمال الجمعية	مخاطر العملية	عدد الاختراقات للشبكة الجمعية/سنوي	مؤشرات أداء العملية
فقدان البيانات		عدد مرات توقف برامج الحماية/سنوي	
الاضرار بالشبكة والسيرفرات والأجهزة		عدد التهديدات الأمنية على الأجهزة / سنوي	
		عدد الثغرات الأمنية للبرامج / سنوي	

### مخطط عملية سلامة وأمن الأجهزة والشبكة الداخلية

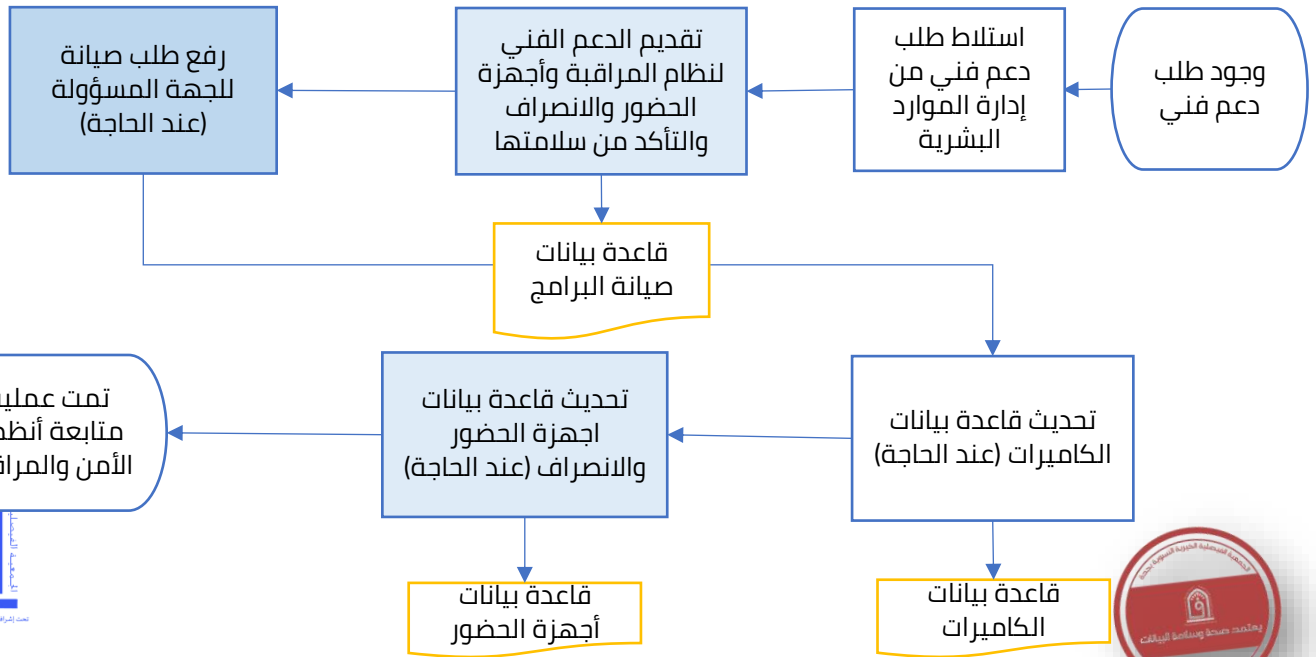


## إدارة التقنية وتكنولوجيا المعلومات

### عملية متابعة أنظمة الأمن والمراقبة

هدف العملية	متابعة أنظمة أمن ومراقبة الجمعية	المسؤول عن تنفيذ العملية	مسؤولية الدعم الفني
المستهدفون من العملية	أنظمة الأمن والمراقبة	الوقت اللازم لتنفيذ العملية	أسبوع عمل
مدخلات العملية	الخطوات الإجرائية للعملية	النموذج/ النظام الإلكتروني	مخرجات العملية
نظام الأمن والمراقبة - نظام الحضور والانصراف	1	البداية: وجود طلب دعم فني من إدارة الموارد البشرية	قاعدة بيانات الكاميرات - قاعة بيانات محدثة
	2	استلام طلب دعم فني من إدارة الموارد البشرية	
	3	تقديم الدعم الفني لنظام المراقبة وأجهزة الحضور والانصراف والتأكد من سلامتها	
	4	رفع طلب صيانة للجهة المسؤولة (عند الحاجة)	
	5	تحديث قاعدة بيانات الكاميرات (عند الحاجة)	
	6	تحديث قاعدة بيانات اجهزة الحضور والانصراف (عند الحاجة)	
مؤشرات أداء العملية	عدد مرات تعطل نظام الأمن والمراقبة/سنوي	مخاطر العملية	التأثير على أمن وسلامة الجمعية التأثير على صرف الرواتب

### مخطط عملية متابعة أنظمة الأمن والمراقبة



## إدارة التقنية وتكنولوجيا المعلومات

### 3.3 سلامة وأمن البيانات

#### 1.3 فتح / إغلاق حساب الموظف

- إدارة الموارد البشرية هي المسؤولة عن فتح/ إغلاق حساب الموظف موضح فيه اسم الموظف باللغة العربية , والمسمى الوظيفي والإدارة التابع لها الموظف.
- إدارة التقنية وتكنولوجيا المعلومات تقوم بإعطاء الصلاحيات المخصصة للموظف حسب مهامه الوظيفية.

#### 2.3 صلاحية الاطلاع على البيانات

##### صلاحيات عامة :

- **المدير العام:** له الحق في الاطلاع على جميع البيانات وما ينتج عنها (معلومات, تقارير).
- **المراجع الداخلي:** له الحق في الاطلاع على جميع البيانات التي تتبع الإدارات وكتابة التقارير عنها .
- **مدير الإدارة:** له الحق في الاطلاع على جميع البيانات التي تقع ضمن نطاق إدارته.
- **رئيس القسم:** له الحق في الاطلاع على جميع البيانات التي تقع ضمن نظام قسمه .
- **الموظف:** له الحق في الاطلاع على جميع البيانات التي تقع ضمن نطاق عمله وصلاحيته.
- **البيانات العامة:** تحدد الجمعية بيانات محددة على أنها عامة يمكن الاطلاع عليها ومشاركتها ونشرها على موقعها الإلكتروني بدون الحاجة إلى إذن معين.

#### 3.3 سلامة وصحة البيانات

- التأكد من إدخال البيانات وصحتها ومسؤولية كل من له عمل يتعلق بإدخال البيانات.
- يعتبر الرئيس المباشر ومدير الإدارة والموظفين المسؤولين عن الإدخالات, مسؤولون مسؤولية مباشرة عن التأكد من صحة الإدخالات وتصحيحها عند الحاجة.
- إدخال البيانات بشكل خاطئ حتى ولو على سبيل تسيير العمل وعدم تعطيله يعتبر تخريباً متعمداً للبيانات وما ينتج عنها, وما قد يترتب عليها من قرارات, ويتحمل مسؤولية ذلك كل من له علاقة مباشرة بذلك

## إدارة التقنية وتكنولوجيا المعلومات

### 4. الأدوار والمسؤوليات

- راعي ومالك وثيقة السياسة: مسؤول تقنية المعلومات.
- مراجعة السياسة وتحديثها: مسؤول تقنية المعلومات.
- تنفيذ السياسة وتطبيقها: المدير التنفيذي ومسؤول تقنية المعلومات وإدارة الموارد البشرية.

### 5. الالتزام بالسياسة

- على مسؤول تقنية المعلومات ضمان التزام الجمعية الفيصالية بهذه السياسة دورياً.
- على إدارة تقنية المعلومات وجميع الإدارات في الجمعية الفيصالية الالتزام بهذه السياسة.
- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب إجراءات المتبعة في الجمعية الفيصالية

## المادة الثانية

# سياسة مواصفات أجهزة الكمبيوتر وملحقاتها والبرمجيات

### بطاقة سياسة مواصفات أجهزة الكمبيوتر وملحقاتها

2025	تاريخ المراجعة	2025/5/18	تاريخ التحديث	10/01/20 23	تاريخ الإصدار	1	رقم الإصدار	IT-08-P2	رمز السياسة
------	-------------------	-----------	------------------	----------------	------------------	---	----------------	----------	----------------

## إدارة التقنية وتكنولوجيا المعلومات

### 1. الأهداف

تحدد هذه السياسة مواصفات أجهزة الكمبيوتر، والبرمجيات بمختلف أنواعها وملحقاتها، لضمان العمل بالشكل المطلوب مع الأنظمة الحالية، ولضمان التوافق فيها بينها

### 2. نطاق العمل

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة بالجمعية الفيصلية، وتطبق على جميع العاملين فيها

### 3. بنود السياسة

**1.3** تقدير الاحتياج الفعلي من الجهاز / البرمجيات قبل الاعتماد والشراء

**2.3** عند شراء الأجهزة يجب أن يكون المورد معتمد مع مراعاة توفر ضمان لا يقل عن سنة، ويفضل أن يكون الضمان لمدة ثلاث سنوات.

### 3.3 يجب أن تحتوي حزمة الكمبيوتر المكتبي على:

- الوحدة الرئيسية، ويمكن أن تكون بشكل برج رأسي، أو بشكل مكتبي أفقي.
- شاشة كمبيوتر لا تقل عن 21 بوصة.
- لوحة مفاتيح قياسية سلكية عربي/إنجليزي.
- فأرة قياسية سلكية.
- البرامج القياسية التالية للجهاز المكتبي:
  - حزمة أوفيس 365 عربية.
  - مضاد فيروسات من نوع أمن . windows
  - أدوبي ريدر .
  - Anydesk برنامج الدعم الفني
- ملحقات الجهاز المكتبي التي تتطلب موافقة الرئيس المباشر وإدارة تقنية المعلومات:
  - لوحة مفاتيح لا سلكية .
  - فأرة لا سلكية .
  - سماعات .
  - مايكروفون .
  - كاميرا ملحقة .
  - طابعة مكتبية .
  - ماسح ضوئي مكتبي .

## إدارة التقنية وتكنولوجيا المعلومات

- يجب أن يكون الحد الأدنى لمواصفات جهاز الكمبيوتر المكتبي كالتالي :
  - المعالج Intel i5 بسرعة لا تقل عن 2 جيجا هيرتز .
  - الذاكرة RAM بحجم لا يقل عن 8 جيجابايت .
  - القرص الصلب لا يقل عن 500 جيجابايت .
  - منفذ شاشة متوافق مع الشاشات المستخدمة في الجمعية .
  - منفذ شبكة بسرعة لا تقل عن 100 ميجابايت .
  - ان لا يقل اصدار ويندوز عن windows 10

### 4.3 أجهزة الكمبيوتر المحمول

- تشمل كل من (لابتوب أو نوت بوك أو التابلت ) .
- يجب شراء أجهزة الكمبيوتر من ماركة معروفة HP , DELL وغيرهما , ومن مورد معتمد , ويجب أن تكون مدعومة بضمان لا يقل عن سنة , ويفضل ضمان ثلاث سنوات .
- توفير نظام التشغيل مايكروسوفت ويندوز 11 نظام 64 بت وحزمة أوفيس حزمة أوفيس 365
- يجب أن يتوافق ويندمج مع الأجهزة الموجودة
- الحد الأدنى لمواصفات الكمبيوتر المحمول كالتالي :
  - المعالج من نوع Intel i5 بسرعة 2 جيجا هيرتز .
  - الذاكرة 8 ميغابايت .
  - منفذ شبكة . Ethernet
  - شبكة لاسلكية .
  - عدد 2 منفذ USB على الأقل .
  - منفذ . HDMI .

### 5.3 أجهزة الخادم/السيرفر

- يجب شراء أنظمة الخادم بواسطة قسم نظم وتقنية المعلومات .
- الخوادم التي يتم شراؤها يجب أن تكون متوافقة مع أجهزة الكمبيوتر وأنظمة التشغيل الأخرى الموجودة في الجمعية .
- يجب أن تكون جميع الخوادم التي يتم شراؤها مدعومة بواسطة ضمان 3 سنوات على الأقل

6.3 أي تغيير على هذه المواصفات يجب أن تتم عن طريق مسؤول التقنية , وبموافقة واعتماد مدير إدارة التقنية وتكنولوجيا المعلومات.

## إدارة التقنية وتكنولوجيا المعلومات

### 7.3 البرمجيات

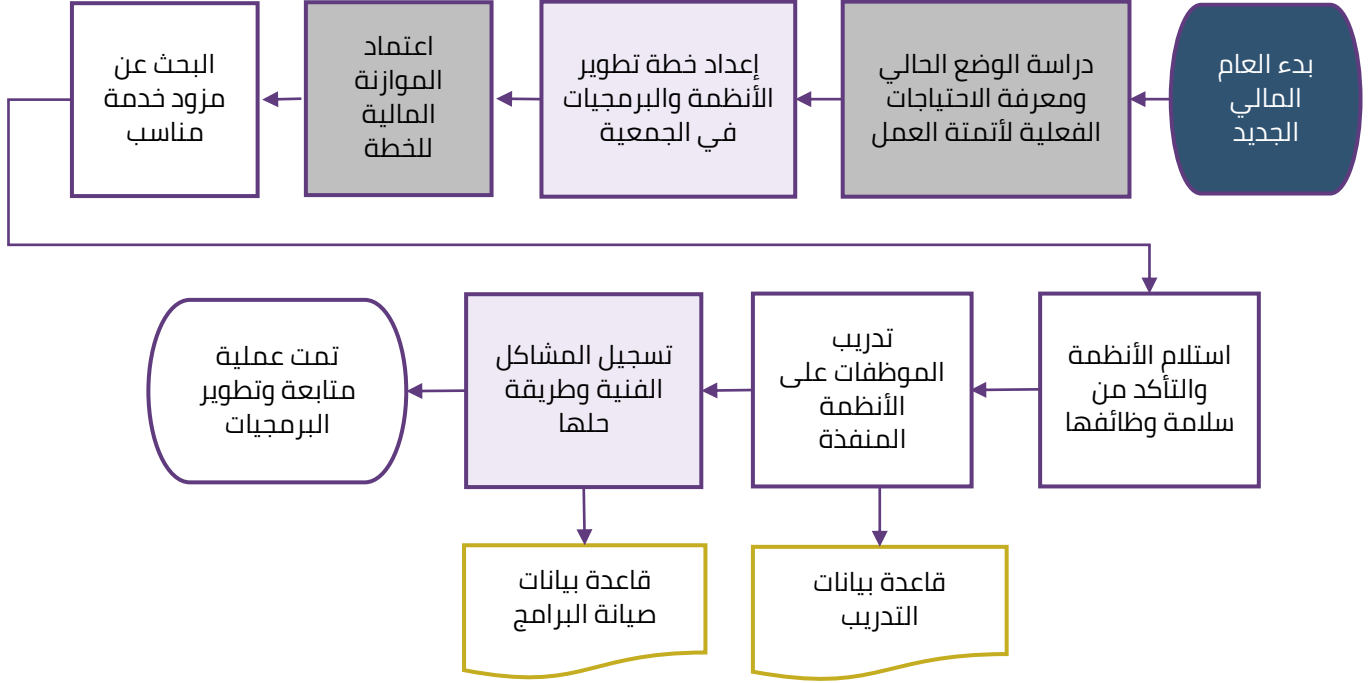
- توفير نسخ أصلية من الأنظمة والبرامج أو الاشتراك بشكل سنوي
- معرفة الاحتياج الفعلي من البرامج المطلوبة والتأكد من تناسب جميع عمليات الأنظمة مع طبيعة عمل وسياسات الجمعية ومع الأجهزة الموجودة ورفع التوصيات بذلك.
- مراعاة بنود أمن وسلامة المعلومات عند التعاقد مع مزودين الخدمة.
- توفير أدلة إجرائية وتدريب العاملين.

### عملية متابعة وتطوير البرمجيات

مسؤولة البرامج والعمليات	المسؤول عن تنفيذ العملية	متابعة وتطوير برمجيات الجمعية	هدف العملية
مستمر	الوقت اللازم لتنفيذ العملية	جميع برمجيات وأنظمة الجمعية	المستهدفون من العملية
مخرجات العملية	النموذج/ النظام الإلكتروني	الخطوات الإجرائية للعملية	مدخلات العملية
- أنظمة إلكترونية - قاعدة بيانات - صيانة البرامج محدثة - تدريب موظفات - أدلة إجرائية		البداية: بدء العام المالي الجديد	1
		دراسة الوضع الحالي ومعرفة الاحتياجات الفعلية لأتمتة العمل المؤسسي في الجمعية، من خلال الاجتماع مع أقسام الجمعية	2
		إعداد خطة تطوير الأنظمة والبرمجيات في الجمعية	3
		اعتماد الموازنة المالية للخطة	4
		البحث عن مزود خدمة مناسب والتعاقد بعد التأكد من تغطية احتياجات الأقسام	5
		استلام الأنظمة والتأكد من سلامة وظائفها ومخرجاتها متابعة أدائها	6
		تدريب الموظفين على الأنظمة المنفذة وتقديم الدعم الفني اللازم	7
		تنفيذ لقاءات مع الأقسام، بهدف تطوير الأنظمة القائمة	8
		في حال وجود مشكلة في النظام يتم التواصل مع فريق الدعم الفني لحلها	9
		تسجيل المشاكل الفنية وطريقة حلها	10
		إعداد أدلة إجرائية للبرامج والمنصات، ونشرها لجميع أقسام الجمعية	11
التأثير على تنفيذ أعمال الجمعية	مخاطر العملية	نسبة الإنجاز من خطة تطوير الأنظمة والبرمجيات	مؤشرات أداء العملية
التأثير على تقديم الخدمة للمستفيد		عدد أيام تدريب الموظفين على الأنظمة والبرمجيات/سنوي	
		عدد ورش عمل تدريب الموظفين على الأنظمة والبرمجيات/سنوي	
		عدد الأنظمة الإلكترونية المفعلة	

## إدارة التقنية وتكنولوجيا المعلومات

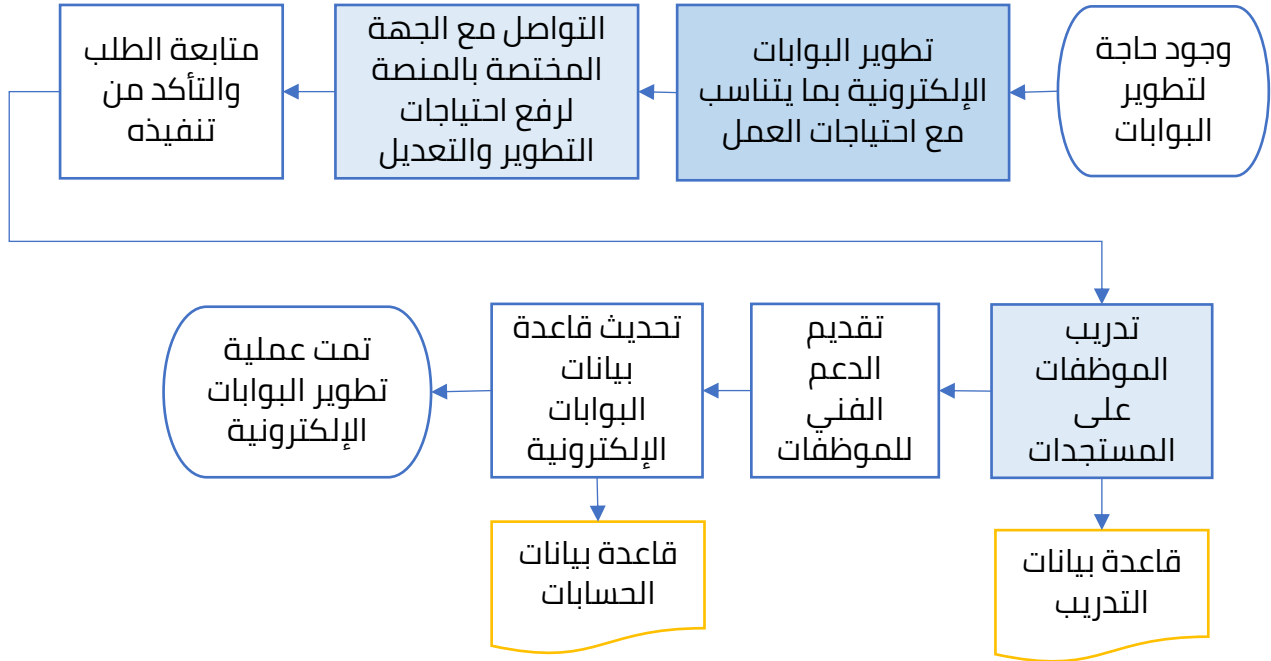
### مخطط عملية متابعة وتطوير البرمجيات



### عملية تطوير البوابات الإلكترونية

هدف العملية	تطوير البوابات الإلكترونية	المسؤول عن تنفيذ العملية	مسؤولية البرامج والعمليات
المستهدفون من العملية	جميع البوابات الإلكترونية للجمعية	الوقت اللازم لتنفيذ العملية	مستمر
مدخلات العملية	الخطوات الإجرائية للعملية	النموذج/ النظام الإلكتروني	مخرجات العملية
بوابات الجمعية الإلكترونية	1	البداية: وجود حاجة لتطوير البوابات الإلكترونية للجمعية	- قاعدة بيانات الحسابات محدثة - تدريب الموظفين - ادلة إجرائية
	2	تطوير البوابات الإلكترونية بما يتناسب مع احتياجات العمل	
	3	التواصل مع الجهة المختصة بالمنصة لرفع احتياجات التطوير والتعديل	
	4	متابعة الطلب والتأكد من تنفيذه	
	5	تدريب الموظفين على المستجدات (ورش عمل وأدلة إجرائية)	
	6	تقديم الدعم الفني للموظفات	
	7	تحديث قاعدة بيانات البوابات الإلكترونية (عند الحاجة)	
مؤشرات أداء العملية	عدد البوابات التي تم تطويرها	مخاطر العملية	التأثير على تنفيذ أعمال الجمعية

## مخطط عملية تطوير البوابات الإلكترونية



### 4. الأدوار والمسؤوليات

- راعي ومالك وثيقة السياسة: مسؤول تقنية المعلومات.
- مراجعة السياسة وتحديثها: مسؤول تقنية المعلومات.
- تنفيذ السياسة وتطبيقها: المدير التنفيذي ومسؤول تقنية المعلومات وإدارة الموارد البشرية

### 5. الالتزام بالسياسة

- على مسؤول تقنية المعلومات ضمان التزام الجمعية الفيصلية بهذه السياسة دورياً.
- على إدارة تقنية المعلومات وجميع الإدارات في الجمعية الفيصلية الالتزام بهذه السياسة.
- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب إجراءات المتابعة في الجمعية الفيصلية

## المادة الثالثة صيانة الأجهزة

### بطاقة سياسة صيانة الأجهزة

2025	تاريخ المراجعة ة	فبراير 2025	تاريخ التحديث	10/01/20 23	تاريخ الإصدار	1	رقم الإصدار	IT-08- P3	رمز السياسة
------	------------------------	----------------	------------------	----------------	------------------	---	----------------	--------------	----------------

## إدارة التقنية وتكنولوجيا المعلومات

### 1. الأهداف

تحدد هذه السياسة الأساليب المتبعة في الجمعية لصيانة الأجهزة بهدف إطالة عمرها الافتراضي والمحافظة على الأصول وضمان سلامة الاستخدام الأمثل

### 2. نطاق العمل

تغطي هذه السياسة جميع الأصول التقنية الخاصة بالجمعية الفيصلية، وتنطبق على جميع العاملين فيها

### 3. بنود السياسة

#### 1.3 الصيانة الوقائية

- يقوم مسؤول تقنية المعلومات بإجراء صيانة وقائية لكل الأجهزة مرة واحدة كل ستة أشهر ورصد التحديثات في قاعدة بيانات الدعم الفني.
- تتضمن عملية الصيانة الوقائية :
  - فحص أداء الجهاز وتحسينه
  - فحص البرمجيات العاملة ونظام التشغيل وتحديثهم .
- وضع خطة سنوية لتحسين الأجهزة من قبل مسؤول تقنية المعلومات

#### 2.3 الصيانة اليومية

- الصيانة اليومية تتضمن مراقبة أوضاع السيرفرات والشبكة والأجهزة , ومعالجة أي مشكلة فور حدوثها .
- تسجل جميع العمليات في قاعدة بيانات الدعم الفني.
- التعاون مع جهات معتمدة لصيانة الاجهزة عند الحاجة

#### 3.3 صيانة الشبكة

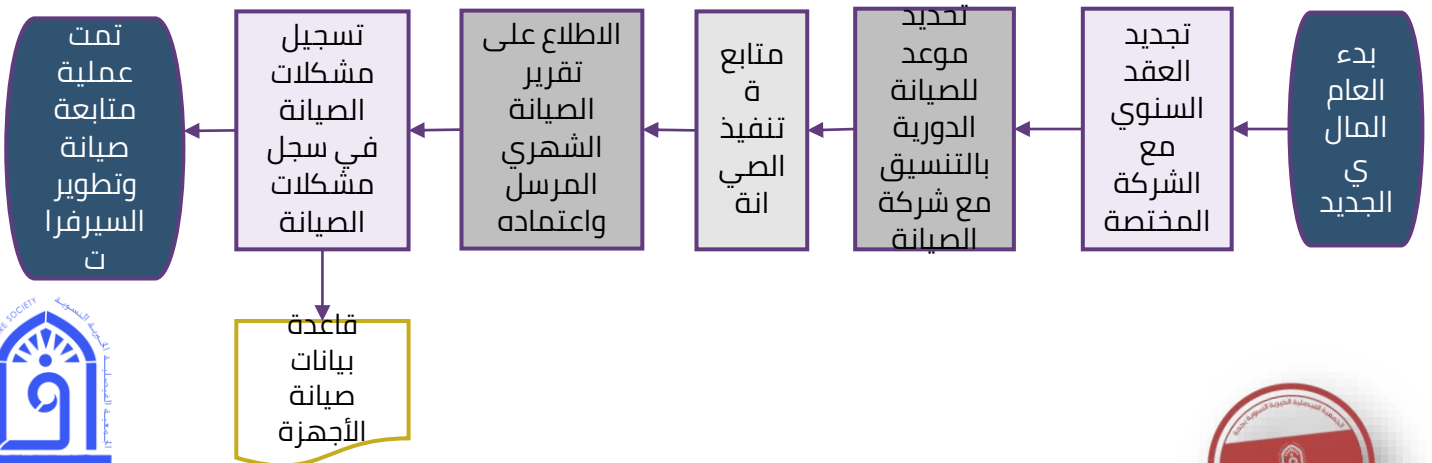
- متابعة مسؤول التقنية لزيارات الشركة المسؤولة لصيانة الشبكة والسيرفرات SLA مرة في الشهر
- معالجة حالات الدعم الفني الطارئة بالتنسيق مع الشركة.
- تسجل جميع العمليات في قاعدة بيانات الدعم الفني.

## إدارة التقنية وتكنولوجيا المعلومات

### عملية متابعة صيانة وتطوير السيرفرات والشبكة الداخلية

هدف العملية	متابعة عملية الصيانة والتطوير	المسؤول عن تنفيذ العملية	مسؤولية الشبكات
المستهدفون من العملية	جميع سيرفرات الجمعية	الوقت اللازم لتنفيذ العملية	أسبوع عمل
مدخلات العملية	الخطوات الإجرائية للعملية	النموذج/ النظام الإلكتروني	مخرجات العملية
عقد - صيانة SLA	1	البداية: بدء العام المالي الجديد	
	2	تجديد العقد السنوي مع الشركة المختصة	عقد الصيانة SLA
	3	مناقشة التوصيات على البنية التحتية إن وجدت مع الشركة المختصة	
	4	التنسيق مع المسؤول في شركة الصيانة لتحديد موعد للصيانة الدورية من كل شهر (مرة الى مرتين في الشهر)	
	5	استقبال مهندس الصيانة في مقر الجمعية في حال كانت الصيانة حضوريا أو عن طريق anyDesk في حالات كانت عن بعد	
	6	متابعة تنفيذ الصيانة	
	7	الاطلاع على تقرير الصيانة الشهري المرسل واعتماده	تقرير SLA
	8	في حال وجود مشكلة يتم فتح تذكرة صيانة مع الشركة عبر موقعهم الإلكتروني	
	9	متابعة التذكرة والتأكد من حل المشكلة، عبر موقع الشركة + البريد الإلكتروني	
	10	تسجيل مشكلات الصيانة في سجل مشكلات الصيانة	قاعدة بيانات صيانة الأجهزة التقنية
مؤشرات أداء العملية	عدد مشاكل الصيانة المنفذة/سنوي عدد مرات تعطل السيرفرات/ الشبكة الداخلية/ سنوي	مخاطر العملية	التأثير على تنفيذ أعمال الجمعية

### مخطط عملية متابعة صيانة وتطوير السيرفرات والشبكة الداخلية



## إدارة التقنية وتكنولوجيا المعلومات

### 4. الأدوار والمسؤوليات

- راعي ومالك وثيقة السياسة: مسؤول تقنية المعلومات.
- مراجعة السياسة وتحديثها: مسؤول تقنية المعلومات.
- تنفيذ السياسة وتطبيقها: المدير التنفيذي ومسؤول تقنية المعلومات وإدارة الموارد البشرية

### 5. الالتزام بالسياسة

- على مسؤول تقنية المعلومات ضمان التزام الجمعية الفيسالية بهذه السياسة دورياً.
- على إدارة تقنية المعلومات وجميع الإدارات في الجمعية الفيسالية الالتزام بهذه السياسة.
- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب إجراءات المتبعة في الجمعية الفيسالية

## المادة الرابعة سياسة الدعم الفني

بطاقة سياسة الدعم الفني									
2025	تاريخ المراجعة عة	فبراير 2025	تاريخ التحديث	10/01/20 23	تاريخ الإصدار	1	رقم الإصدار	IT-08- P4	رمز السياسة

## إدارة التقنية وتكنولوجيا المعلومات

### 1. الأهداف

تحدد هذه السياسة ضوابط تقديم الدعم الفني وقنوات التواصل المتاحة

### 2. نطاق العمل

تغطي هذه السياسة جميع الأصول التقنية والبرمجيات الخاصة بالجمعية الفيصلية، وتنطبق على جميع العاملين فيها

### 3. بنود السياسة

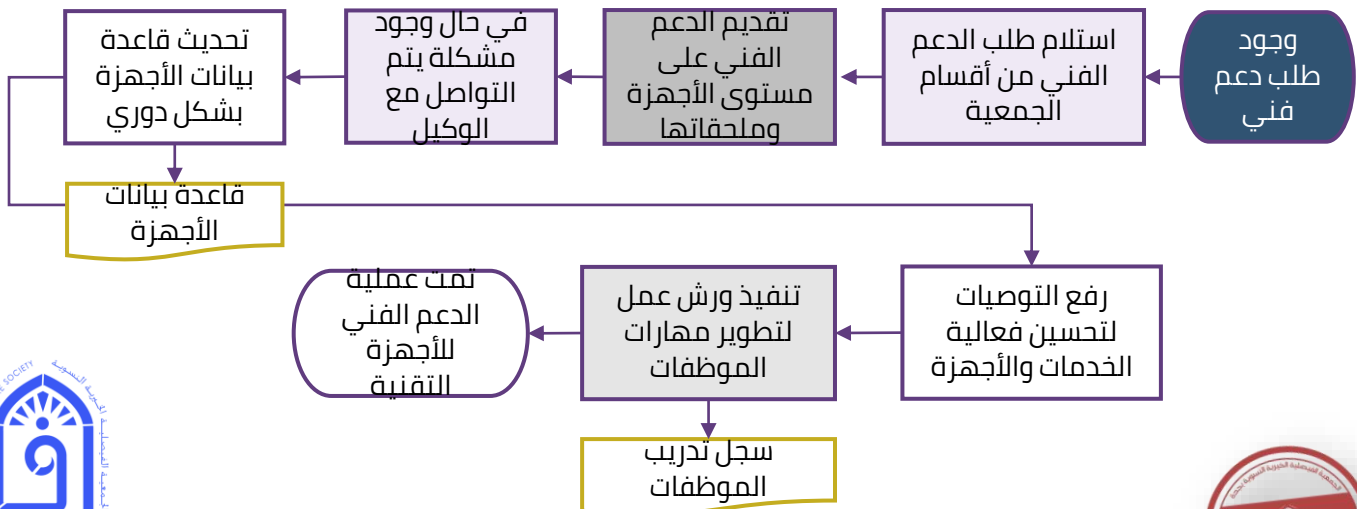
#### 1.3 الدعم الفني الداخلي

- توفير أدوات وآليات مناسبة لرصد طلبات الدعم الفني.
- توفير أدوات مناسبة ومرنة للدعم الفني عن بعد لحل المشكلات التقنية التي تواجه المستخدمين
- تقديم الدعم الفني المباشر لحل المشكلات التقنية التي تواجه المستخدمين.
- في حال تعذر حل المشكلة من خلال فريق الدعم الفني الداخلي يتم الاستعانة في التنفيذ بطرف خارجي.

#### 2.3 الدعم الفني الخارجي

- طلب دعم فني خارجي من جهة ذات خبرة ومعتمدة عند الحاجة.
- متابعة حل المشكلة وإعطاء تغذية راجعة لمقدم الطلب واستكمال إجراءات إغلاقه.
- تسجل جميع العمليات في قاعدة بيانات الدعم الفني.

### مخطط عملية الدعم الفني للأجهزة التقنية



## إدارة التقنية وتكنولوجيا المعلومات

### عملية الدعم الفني للأجهزة التقنية

هدف العملية	تقديم الدعم الفني للأجهزة التقنية وملحقاتها	المسؤول عن تنفيذ العملية	مسؤولية الدعم الفني
المستهدفون من العملية	جميع الأجهزة التقنية في أقسام الجمعية	الوقت اللازم لتنفيذ العملية	مستمر
مدخلات العملية	الخطوات الإجرائية للعملية	النموذج/ النظام الإلكتروني	مخرجات العملية
- طلبات الدعم الفني للأجهزة التقنية	1	البداية: وجود طلب دعم فني	- قاعدة بيانات الأجهزة التقنية محدثة - قاعدة بيانات حسابات الموظفين محدثة - سجل تدريب الموظفين - دليل إجرائي
	2	استلام طلب الدعم الفني من أقسام الجمعية	
	3	تقديم الدعم الفني على مستوى الأجهزة وملحقاتها	
	4	في حال وجود مشكلة يتم التواصل مع الوكيل	
	5	تحديث قاعدة بيانات الأجهزة بشكل دوري	
	6	تحديث قاعدة بيانات حسابات الموظفين	
	7	رفع التوصيات لتحسين فعالية الخدمات والأجهزة	
	8	تنفيذ ورش عمل لتطوير مهارات الموظفين فيما يتعلق بالدعم الفني وكيفية استخدام الأجهزة وملحقاتها	
	9	إعداد سياسات وضوابط لكيفية الاستخدام للأجهزة وملحقاتها، وتعميمها على الجميع	
مؤشرات أداء العملية	متوسط الفترة الزمنية المستغرقة لتقديم الدعم الفني عدد ورش العمل والدورات في تدريب الموظفين على الأجهزة	مخاطر العملية	التأثير على تنفيذ أعمال الجمعية

## إدارة التقنية وتكنولوجيا المعلومات

### سجلات ونماذج عمل العملية

م	رقم النموذج	Form Code	اسم النموذج	فترة الحفظ (سنة)	مسؤولية الحفظ
1	تقنية - نموذج رقم (1)	IT-08-F1	قاعدة بيانات صيانة الأجهزة التقنية	3 سنوات	إدارة تقنية المعلومات
2	تقنية - نموذج رقم (2)	IT-08-F2	قاعدة بيانات التدريب	3 سنوات	إدارة تقنية المعلومات
3	تقنية - نموذج رقم (3)	IT-08-F3	قاعدة بيانات صيانة البرامج	3 سنوات	إدارة تقنية المعلومات
4	تقنية - نموذج رقم (4)	IT-08-F4	قاعدة بيانات الأجهزة	3 سنوات	إدارة تقنية المعلومات
5	تقنية - نموذج رقم (5)	IT-08-F5	قاعدة بيانات حسابات الموظفين	3 سنوات	إدارة تقنية المعلومات
6	تقنية - نموذج رقم (6)	IT-08-F6	لوحة تحكم نظام النسخ الاحتياطي	3 سنوات	إدارة تقنية المعلومات
7	تقنية - نموذج رقم (7)	IT-08-F7	قاعدة بيانات الكاميرات	3 سنوات	إدارة تقنية المعلومات
8	تقنية - نموذج رقم (8)	IT-08-F8	قاعدة بيانات أجهزة الحضور	3 سنوات	إدارة تقنية المعلومات

#### 4. الأدوار والمسؤوليات

- راعي ومالك وثيقة السياسة: مسؤول تقنية المعلومات.
- مراجعة السياسة وتحديثها: مسؤول تقنية المعلومات.
- تنفيذ السياسة وتطبيقها: المدير التنفيذي ومسؤول تقنية المعلومات وإدارة الموارد البشرية

#### 5. الالتزام بالسياسة

- على مسؤول تقنية المعلومات ضمان التزام الجمعية الفيصلية بهذه السياسة دورياً.
- على إدارة تقنية المعلومات وجميع الإدارات في الجمعية الفيصلية الالتزام بهذه السياسة.
- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب إجراءات المتبعة في الجمعية الفيصلية

## المادة الخامسة

# قواعد الأمن والسلامة تجاه التقنية

### وثيقة تعهد-الإصدار الثاني 2023

#### بطاقة سياسة الدعم الفني

2025	تاريخ العرا ة	فبراير 2025	تاريخ التحديث	17/9/2025	تاريخ الإصدار	1	رقم الإصدار	IT-08 - p5	رمز السياسة
------	---------------------	----------------	------------------	-----------	------------------	---	----------------	---------------	----------------

## إدارة التقنية وتكنولوجيا المعلومات

### الجمعية والتقنية

انطلاقاً من الإيمان الراسخ بأهمية التحول الرقمي وتعزيز قدرات الجمعية الرقمية من خلال توفير بيئة عمل محفزة وذات إنتاجية بما يتماشى مع احتياجاتها التطويرية لمواكبة كل جديد بذلت الجمعية جهوداً كبيرة ساهمت في تحقيق نقلات نوعية على مدار الأعوام الماضية، لتطبيق التقنيات الحديثة ضمن استراتيجيات متكاملة ومتوافقة مع أطر ولوائح الجمعية وقيمها الجوهرية.

### حساب الموظف

إدارة الموارد البشرية هي المسؤولة عن فتح حساب الموظف موضح فيه اسم الموظف باللغة العربية، والمسمى الوظيفي والإدارة التابع لها الموظف، وعلى أن يقوم بإرسال بريد إلكتروني إلى إدارة التقنية وتكنولوجيا المعلومات لإعطاء الصلاحيات المخصصة للموظف حسب مهامه الوظيفية.

### مسؤولية الموظف عن حسابه

- بمجرد استلام الموظف لحسابه واستخدامه لأول مرة، يصبح مسؤولاً مسؤولاً كاملة وقانونية عن كل الأعمال التي تحدث في الأنظمة باستخدام هذا الحساب.
- يمنع الموظف من الإفصاح لأحد عن معلومات حسابه (اسم المستخدم وكلمة المرور)، ولا يسمح أن يمكّن أحد من العمل باستخدام حسابه.
- استخدام حساب موظف آخر بدون علمه يعتبر جريمة إلكترونية يعاقب عليها القانون في السعودية.
- عند ضرورة استخدام جهاز موظفة متغيب أو في اجازة يكون ذلك بموافقة من المدير المباشر وتحت إشراف إدارة الموارد البشرية
- كلمة المرور يجب أن تكون سرية ولا يطلع عليها أحد، ولا تكتب في ورقة أو ما شابه، وإنما تحفظ فقط.
- يمنع مشاركة كلمة المرور مع آخرين، حتى مع موظفي تقنية المعلومات إلا في حال كانت هناك مشكلة لدى الموظف في حسابه.
- لا تتحدث عن كلمة المرور من حيث طولها أو تعقيدها مع أحد من خارج نطاق عمل الجمعية.
- عدم استخدام حسابات الجمعية في مواقع إلكترونية لغرض شخصي

## إدارة التقنية وتكنولوجيا المعلومات

### كلمات المرور

- كلمة المرور يجب ألا تقل عن 6 حروف , ويجب أن تحتوي على رمز واحد على الأقل (مثلاً: !@#\$%^&\*)
- كلمة المرور يجب أن تكون سرية ولا يطلع عليها أحد, ولا تكتب في ورقة أو ما شابه, وإنما تحفظ فقط .
- يمنع مشاركة كلمة المرور مع آخرين , حتى مع موظفي تقنية المعلومات إلا في حال كانت هناك مشكلة لدى الموظف في حسابة .

### طلب صلاحية إطلاع على بيانات وما ينتج عنها:

- في حال الرغبة في الاطلاع أو استخدام بيانات وما ينتج عنها لا تقع ضمن حدود صلاحياتك فعليك طلبها من صاحب الصلاحية حسب التسلسل الإداري المعتمد وببريد رسمي
- في حال كان السماح بالاطلاع على البيانات محدد بمدة أو بمهمة, فيجب على الموظف إبلاغ من يلزم بإزالة الصلاحيات المؤقتة.

### المسؤولية عن البيانات وما ينتج عنها :

- كل حسب موقعه يحق له الاطلاع واستخدام البيانات المخول بها, بهدف تحقيق مصلحة ومنفعة للجمعية.
- لا يجوز استخدام هذه البيانات, وما ينتج عنها خارج الجمعية إلا بإذن من صاحب الصلاحية .
- لا يحق نشر هذه البيانات, وما ينتج عنها إلا باعتماد صاحب الصلاحية .

## إدارة التقنية وتكنولوجيا المعلومات

- الكشف عن هذه البيانات وما ينتج عنها لا يتم إلا للمخولين بكشفها, أو نشرها بأي وسيلة.
- الجمعية تحدد طرق النشر المناسبة , والأشخاص المخولين بالنشر , ونوعية البيانات التي تنشر .

### نشر البيانات وما ينتج عنها :

- جميع البيانات التي تمتلكها الجمعية تعتبر أصل ثمين بالغ الأهمية.
- على جميع العاملين في الجمعية ضمان عدم التفريط, أو الإضرار بهذا الأصل بكل ما يملكون من جهد.

### قواعد الأمن والسلامة لغرفة السيرفر:

- يمنع منعاً باتاً الاقتراب من معدات السيرفر إلا من قبل مسؤولة التقنية.
- إغلاق غرفة السيرفر. وتحديد أشخاص مخولين بالدخول
- المحافظة على درجة حرارة الغرفة منخفضة وعدم تعريض السيرفر للحرارة والرطوبة والسوائل.
- التأكد من سلامة المكيفات وجدولة عملية تشغيلهم على التوالي.
- تزويد الغرفة بطفاية حريق.
- عدم استخدام غرفة السيرفر للتخزين.
- التأكد من سلامة التيار الكهربائي وعدم انقطاعه.
- عدم إغلاق الأجهزة ومحولات الطاقة الخاصة بالسيرفر.
- إبلاغ المسؤولين في حالة وجود رائحة التماس كهربائي.
- مراجعة ضوابط الأمن والسلامة بصورة دورية والتأكد من الصيانة الوقائية شهرياً.

### قواعد الأمن والسلامة للأجهزة وملحقاتها:

- عدم وضع المأكولات والمشروبات بالقرب من الأجهزة.
- عدم وضع أي جهاز تحت التكييف مباشرة لتفادي تسرب الماء.
- عدم تحريك الأجهزة من مكانها إلا بعد التواصل مع إدارة التقنية.
- إغلاق الأجهزة بالطريقة الصحيحة بعد الانتهاء من استخدامها .

## إدارة التقنية وتكنولوجيا المعلومات

- عدم فصل الجهاز عند ظهور رسالة تفيد بوجود تحديثات خاصه بالنظام عند إغلاق الجهاز.
- عدم استخدام وحدة تخزين خارجية (مثل: فلاش ميموري- هارديسك- جوال) دون موافقة إدارة التقنية بذلك.
- عدم تجاهل رسائل تحديثات النظام ومزامنة لملفات ومراجعة إدارة التقنية عند الحاجة إبلاغ المسؤولين في حالة وجود رائحة التماس كهربائي.
- عدم تحميل محولات الكهرباء أكثر من طاقتها .
- استخدام محولات وتوصيلات كهربائية ذات نوعية جيدة.
- أهمية حفظ الملفات المهمة في القرص(D)مما يمكننا من المحافظة على الملفات الموجود بالجهاز والتمكن من استعادتها في حال تعطل الجهاز.
- عدم تحميل أي ملفات غير موثوقة من الإنترنت أو البريد الإلكتروني.
- المحافظة على برودة الغرفة وعدم تعريض الجهاز للحرارة، والرطوبة، والسوائل، والأحمال.
- عدم نزع أحد الكابلات من مكانه أثناء عمل الجهاز.
- عدم محاولة فتح الاجهزة بأدوات حادة في حال توقفها عن العمل
- تفريغ ملف المشاركة ( الشير) الخاص بكل موظفة مرة في الأسبوع على الأقل.
- مراجعة ضوابط الأمن والسلامة بصورة دورية والتأكد من الصيانة الوقائية شهرياً.
- تنبيه: الإنترنت مراقب في جميع الأجهزة.

**لذا كان الزاماً على جميع العاملين في الجمعية الالتزام بجميع ما ذكر في هذه الوثيقة وفي حال مخالفة اي بند مذكور سيكون معرض للمساءلة**

التوقيع .....

التاريخ .....

الاسم .....

الوظيفة .....

## المادة السادسة

# سياسة استخدام أدوات الذكاء الاصطناعي التوليدي

بطاقة سياسة الدعم الفني									
2025	تاريخ المراجعة	10/ 6 2025/	تاريخ التحديث	17/9/2025	تاريخ الإصدار	1	رقم الإصدار	IT-08 - p6	رمز السياسة

## إدارة التقنية وتكنولوجيا المعلومات

### 1. الأهداف

تهدف هذه السياسة إلى تنظيم استخدام أدوات وتقنيات الذكاء الاصطناعي التوليدي داخل الجمعية، بما يضمن الكفاءة والابتكار مع الالتزام التام بالأنظمة والسياسات الوطنية الصادرة عن الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA).

الذكاء الاصطناعي التوليدي: هو فرع من فروع الذكاء الاصطناعي يعتمد على تقنيات تعلم الآلة والشبكات العصبية العميقة لمحاكاة قدرة الإنسان على إنتاج بيانات ومحتوى أصيل.

### نطاق العمل

تطبق هذه السياسة على جميع موظفي الجمعية، والمتعاقدين معها، وأي أطراف تستخدم أنظمة الذكاء الاصطناعي ضمن أعمال الجمعية أو مشاريعها.

### 3. بنود السياسة

#### 1.3 المبادئ العامة

- **النزاهة والإنصاف:** تعتمد الجمعية على الذكاء الاصطناعي التوليدي في إعداد تقارير أو مواد توعوية ويجب أن تكون خالية من أي محتوى متحيز أو يضر بسمعة الفئات المستفيدة من خدمات الجمعية.
- **الموثوقية والسلامة:** عند استخدام أدوات الذكاء الاصطناعي التوليدي لإنتاج محتوى (مثل ملخصات أو خطط عمل) تلتزم الجمعية بالتحقق البشري من دقة المخرجات قبل اعتمادها رسمياً.
- **الشفافية وقابلية التفسير:** عند الاستعانة بالذكاء الاصطناعي التوليدي في صياغة وثائق أو إعداد تقارير يجب توضيح أن الأداة التقنية كانت جزءاً من العملية، مع ضمان إمكانية مراجعة وتفسير المخرجات.
- **المساءلة والمسؤولية:** أي موظف يستخدم تقنيات الذكاء الاصطناعي التوليدي في عمله داخل الجمعية مسؤول عن التأكد من دقة وصحة المخرجات، وتحمل الإدارة مسؤولية الرقابة والإشراف.
- **الخصوصية والأمان:** تمنع الجمعية إدخال بيانات شخصية أو حساسة تخص المستفيدين أو المتبرعين في الأدوات العامة للذكاء الاصطناعي التوليدي حفاظاً على سرية المعلومات.
- **الإنسانية:** تلتزم الجمعية بأن يكون الذكاء الاصطناعي التوليدي أداة مساندة تدعم الموظفين في أداء أعمالهم دون أن يحل محل القرارات الإنسانية أو المهنية.
- **المنافع الاجتماعية والبيئية:** تستثمر الجمعية في توظيف الذكاء الاصطناعي التوليدي بطرق تعزز دورها المجتمعي (مثل إعداد محتوى توعوي، أو تطوير حملات تسويقية خيرية) بما يحقق منفعة عامة ويحافظ على القيم البيئية والاجتماعية.

## إدارة التقنية وتكنولوجيا المعلومات

### 2.3 ضوابط الاستخدام

- يحظر استخدام أدوات الذكاء الاصطناعي التوليدي في إنشاء أو نشر محتوى غير لائق أو مخالف للقوانين.
- يمنع إدخال البيانات المالية، الصحية، أو الشخصية الحساسة إلا بعد الحصول على الموافقات الرسمية وضمان حماية البيانات.
- استخدام الأدوات الموثوقة والمعتمدة فقط، ويفضل الأدوات الوطنية أو المرخصة.
- أي مشروع يعتمد على الذكاء الاصطناعي التوليدي يجب أن يخضع للمراجعة التقنية والمصادقة من الإدارة المختصة.

### 3.3 الأمن والخصوصية

- الالتزام بتشفير البيانات عند استخدامها أو تخزينها.
- اتباع سياسات الجمعية لأمن المعلومات بجانب متطلبات الهيئة السعودية للبيانات والذكاء الاصطناعي.

### 4. الأدوار والمسؤوليات

- راعي ومالك وثيقة السياسة: مسؤول تقنية المعلومات.
- مراجعة السياسة وتحديثها: مسؤول تقنية المعلومات.
- تنفيذ السياسة وتطبيقها: المدير التنفيذي ومسؤول تقنية المعلومات وإدارة الموارد البشرية

### 5. الالتزام بالسياسة

- تلتزم الجمعية بتوفير برامج تدريبية وتوعوية لجميع الموظفين حول الاستخدام الآمن والمسؤول لأدوات الذكاء الاصطناعي التوليدي.
- على إدارة تقنية المعلومات وجميع الإدارات في الجمعية الفيصلية الالتزام بهذه السياسة.
- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب إجراءات المتبعة في الجمعية الفيصلية

## إدارة التقنية وتكنولوجيا المعلومات

### المرجع:

### مراجعة واعتماد أصحاب الصلاحية :

تحديث لوائح وسياسات وأنظمة الجمعية الفيصلية  
عُرض في مجلس الإدارة الجلسة رقم (5) بتاريخ 1446/11/20 هـ الموافق 2025/5/18م  
ضمن جدول الأعمال ( بند رقم 5) الاطلاع على تقارير اللجان للربع الأول ومناقشة واعتماد توصيات  
لجنة المراجعة الداخلية .

"تم الاطلاع واعتماد هذه السياسة والعمل بموجبها من تاريخ الاعتماد"

### توقيع واعتماد مجلس الإدارة

الترتيب	الأسماء	التوقيع
1.	الأستاذة خيرية محمد نوررحيمي	
2.	الدكتورة. عبلة عبد الحميد بخاري	
3.	الأستاذة فاطمة محمد علي فارسي	
4.	الدكتورة. مريم عبد الله الصبان	
5.	أستاذة دكتور. سمر محمد السقايف	
6.	الدكتورة. سهى محمد علاوي	
7.	الأستاذة. عبير غازي جليد ان	
8.	الدكتورة. ندى عمر العولقي	
9.	الدكتورة. هلا عبد الله السقايف	
10.	الدكتورة. ربا خالد شيرة	
11.	الأستاذة. رجاء عبد الرحمن محمد مؤمنه	
12.	أستاذة دكتور. لنا أحمد شيتاوي	
13.	الأستاذة. خلود أحمد شيتاوي	