اعتدال
للتكافل والاستدامة
ETEDAL SOLIDARITY & SUSTAINABILITY

سياســـــات وحـــدة
تقنيـــــة المعلومات

معتمد
2026-07-13

بالاعتدال تشكر النعم وتستدام

Etedal.org.sa


بسم الله الرحمن الرحيم

المحتويات :

سياسات وحدة تقنية المعلومات

بيانات ضبط الوثيقة

- اسم الوثيقة: سياسات وحدة تقنية المعلومات
- الجهة المالكة: وحدة تقنية المعلومات
- جهة الاعتماد: مجلس الإدارة
- رقم الإصدار: الإصدار الأول
- تاريخ الاعتماد : 17 فبراير 2026م
- تاريخ السريان: من تاريخ الاعتماد
- مستوى السرية: للاستخدام الداخلي
- حالة الوثيقة: مسودة

1. مقدمة

انطلاقًا من حرص جمعية اعتدال للتكافل والاستدامة على حماية أصولها الرقمية ورفع موثوقية خدماتها التقنية، وتعزيز الامتثال والحوكمة المؤسسية، تم إعداد هذه السياسات لتكون مرجعًا تنظيميًا مُعتمدًا يُوحِّد الممارسات ويضبط أسلوب إدارة وتشغيل واستخدام الأنظمة والأصول التقنية داخل الجمعية.
وتأتي هذه السياسات لحماية البيانات وضمان أمنها وفق مبادئ الأمن السيبراني الأساسية: السرية، والسلامة، والتوافر، وبما يدعم استمرارية الأعمال ويحافظ على ثقة المستفيدين والداعمين والشركاء.

2. الهدف من السياسات

تهدف هذه السياسات إلى:

1. وضع إطار حوكمة واضح لإدارة تقنية المعلومات وتحديد المسؤوليات والصلاحيات.
2. حماية بيانات الجمعية والمستفيدين والشركاء من المخاطر التقنية والتهديدات السيبرانية.
3. تنظيم الاستخدام المقبول للأصول التقنية والبريد الإلكتروني والأجهزة والأنظمة والصلاحيات.
4. تعزيز جاهزية الجمعية لاستمرارية الأعمال والتعافي من الكوارث والاستجابة للحوادث.
5. رفع كفاءة التشغيل وتحسين جودة الخدمات التقنية عبر إجراءات موحدة قابلة للقياس والمراجعة.

3. نطاق التطبيق

تسري هذه السياسات على جميع منسوبي الجمعية (الموظفين والمتطوعين والمتعاونين) وكل من يتم منحه صلاحية أو وصولًا إلى أنظمة الجمعية أو بياناتها أو أصولها التقنية، بما يشمل الأجهزة والشبكات والبريد الإلكتروني والأنظمة وقواعد البيانات والخدمات السحابية.

4. الاعتماد والالتزام

يُعد اعتماد هذه السياسات من مجلس الإدارة مرجعية ملزمة، ويترتب على جميع الأطراف الالتزام بما ورد فيها، وتقوم الإدارة التنفيذية ووحدة تقنية المعلومات بمتابعة التطبيق ورفع التقارير اللازمة وفق ما تقتضيه الحاجة.

أولاً : سياسة أمن البريد الإلكتروني

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة **بحماية البريد الإلكتروني لجمعية اعتدال** من المخاطر السيبرانية والتهديدات الداخلية والخارجية، ويتم ذلك من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.
وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم 2-4-1 من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع أنظمة البريد الإلكتروني الخاصة بجمعية اعتدال وتنطبق على جميع العاملين في **جمعية اعتدال.**

بنود السياسة

1. يجب توفير تقنيات حديثة لحماية البريد الإلكتروني وتحليل وتصفية (Filtering) رسائل البريد الإلكتروني وحظر الرسائل المشبوهة، مثل الرسائل الاقتحامية (Spam Emails) ورسائل التصيّد الإلكتروني (Phishing Emails).
2. يجب أن تستخدم أنظمة البريد الإلكتروني أرقام تعريف المستخدم وكلمات المرور مرتبطة، لضمان عزل اتصالات المستخدمين المختلفين.
3. يجب توفير التقنيات اللازمة لتشفير البريد الإلكتروني الذي يحتوي على معلومات مصنفة.
4. يجب تحديد مسؤولية البريد الإلكتروني للحسابات العامة والمشتركة.
5. يجب توفير تقنيات الحماية اللازمة من الفيروسات، والبرمجيات الضارة غير المعروفة مسبقاً (Zero-Day Protection) على خوادم البريد الإلكتروني؛ والتأكد من فحص الرسائل قبل وصولها لصندوق بريد المستخدم.
6. يجب توثيق مجال البريد الإلكتروني لجمعية اعتدال عن طريق استخدام الوسائل اللازمة؛ مثل طريقة إطار سياسة المرسل (Sender Policy Framework) لمنع تزوير البريد الإلكتروني (Email Spoofing). كما يجب التأكد من موثوقية مجالات رسائل البريد الواردة (Incoming message DMARC verification).
7. يجب أن يقتصر الوصول إلى رسائل البريد الإلكتروني على العاملين لدى **جمعية اعتدال.**
8. يجب اتخاذ الإجراءات اللازمة؛ لمنع استخدام البريد الإلكتروني **لجمعية اعتدال** في غير أغراض العمل.
9. يمنع وصول مسؤول النظام (System Administrator) إلى معلومات البريد الإلكتروني الخاصة بأي موظف دون الحصول على تصريح مسبق.
10. يجب تحديد حجم مرفقات البريد الإلكتروني الصادر والوارد، وسعة صندوق البريد لكل مستخدم. وكذلك العمل على الحد من إتاحة إرسال الرسائل الجماعية لعدد كبير من المستخدمين.
11. يجب تذييل رسائل البريد الإلكتروني المرسلة إلى خارج جمعية اعتدال بإشعار إخلاء المسؤولية.

12. يجـب تطبيق التقنيـات اللازمة؛ لحماية سرية رسـائل البريد الإلـكتروني وسلامتها، وتوافرهـا أثناء نقلها وحفظها؛ وتشمل هذه الإجراءات استخدام تقنيات التشفير وتقنيات منع تسريب البيانات.
13. يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لنظام البريد الإلكتروني.
14. يجب تعطيل خدمة تحويل البريد الإلكتروني من الخادم (Open Mail Relay).

الأدوار والمسؤوليات

1. راعي ومالك وثيقة السياسة:مدير إدارة تقنية المعلومات.
2. مراجعة السياسة وتحديثها: إدارة تقنية المعلومات.
3. تنفيذ السياسة وتطبيقها: إدارة تقنية المعلومات.

الالتزام بالسياسة

1. يجب على مدير إدارة تقنية المعلومات ضمان التزام **جمعية اعتدال** بهذه السياسة بشكل دوري.
2. يجب على جميع العاملين في **جمعية اعتدال** الالتزام بهذه السياسة.
3. قـد يُعرض أي انتهاك لهذه السياسـة صاحب المخالفة إلى إجراء تأديبي؛ حسـب الإجـراءات المتبعة في **جمعية اعتدال.**

ثانياً : سياسة أمن أجهزة المستخدمين والأجهزة المحمولة

الأهداف

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لتقليل المخاطر السيبرانية الناتجة عن استخدام أجهزة المستخدمين (Workstations)، والأجهزة الشخصية للعاملين (BYOD "Bring Your Own Device") داخل **جمعية اعتدال**، وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي سرية المعلومات وسلامتها وتوافرها.
تتبع هذه السياسة المتطلبات التشريعية والتنظيمية الوطنية وأفضل الممارسات الدولية ذات العلاقة، وهي متطلب تشريعي كما هو مذكور في الضوابط رقم 2-3-1 و2-6-1 من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع أجهزة المستخدمين والأجهزة المحمولة للعاملين داخل **جمعية اعتدال** وتنطبق على جميع العاملين في **جمعية اعتدال.**

بنود السياسة

1. البنود العامة

- 1-1 يجب حماية البيانات والمعلومات المُخزّنة في أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية (BYOD) حسب تصنيفها باستخدام الضوابط الأمنية المناسبة لتقييد الوصول إلى هذه المعلومات، ومنع العاملين غير المصرّح لهم من الوصول لها أو الاطلاع عليها.
- 1-2 يجب تحديث برمجيات أجهزة المستخدمين والأجهزة المحمولة، بما في ذلك أنظمة التشغيل والبرامج والتطبيقات، وتزويدها بأحدث حزم التحديثات والإصلاحات وذلك وفقاً لسياسة إدارة التحديثات والإصلاحات المعتمدة في **جمعية اعتدال.**
- 1-3 يجب تطبيق ضوابط الإعدادات والتحصين (Configuration and Hardening) لأجهزة المستخدمين والأجهزة المحمولة وفقاً لمعايير الأمن السيبراني.
- 1-4 يجب عدم منح العاملين صلاحيات هامة وحساسة (Privileged Access) على أجهزة المستخدمين والأجهزة المحمولة، ويجب منح الصلاحيات وفقاً لمبدأ الحد الأدنى من الصلاحيات والامتيازات.
- 1-5 يجب حذف أو إعادة تسمية حسابات المستخدم الافتراضية في أنظمة التشغيل والتطبيقات.
- 1-6 يجب مزامنة التوقيت (Clock Synchronization) مركزياً ومن مصدر دقيق وموثوق لجميع أجهزة المستخدمين والأجهزة المحمولة.
- 1-7 يجب تزويد أجهزة المستخدمين والأجهزة المحمولة برسالة نصيّة (Banner) لإتاحة الاستخدام المصرّح به.
- 1-8 يجب السماح فقط بقائمة محددة من التطبيقات (Application Whitelisting) ومنع تسرّب البيانات (Data Leakage Prevention) واستخدام أنظمة مراقبة البيانات وغيرها.

- 1-9 يجب تشـفير وسـائط التخزين الخاصة بأجهزة المسـتخدمين والأجهزة المحمولة الهامة والحساسة والتي لها صلاحيات متقدمة وفقاً لمعيار التشفير المعتمد في **جمعية اعتدال.**
- 1-10 يجب منع اسـتخدام وسـائط التخزين الخارجية، ويجب الحصول على إذن مسبق من إدارة تقنية المعلومات لامتلاك صلاحية استخدام وسائط التخزين الخارجية.
- 1-11 يجـب عدم السـماح لأجهـزة المسـتخدمين والأجهـزة المحمولة والأجهزة الشـخصية (BYOD) المزوّدة ببرمجيات غير محدثة أو منتهية الصلاحية (بما في ذلك أنظمة التشغيل والبرامج والتطبيقـات) بالاتصال بشـبكة جمعية اعتدال لمنـع التهديدات الأمنية الناشـئة عن البرمجيات منتهية الصلاحية غير المحمية بحزم التحديثات والإصلاحات.
- 1-12 يجب أن تُمنَع أجهزة المسـتخدمين والأجهزة المحمولة والأجهزة الشخصية (BYOD) غير المـزوّدة بأحدث برمجيات الحماية من الاتصال بشـبكة **جمعية اعتدال** لتجنب حدوث المخاطر السـيبرانية التي تؤدي إلى الوصول غير المصرّح به أو دخول البرمجيات الضارة أو تسرّب البيانات. وتتضمّن برمجيات الحماية برامج إلزامية، مثل: برامج الحماية من الفيروسات والبرامج والأنشطة المشـبوهة والبرمجيـات الضـارة (Malware)، وجـدار الحماية للمسـتضيف (Host-Based Firewall)، وأنظمـة الحمايـة المتقدمـة لاكتشـاف ومنـع الاختراقـات في المسـتضيف (Host-based Intrusion Detection/Prevention).
- 1-13 يجـب ضبط إعدادات أجهزة المسـتخدمين والأجهزة المحمولة غير المسـتخدمة بحيث تعرض شاشـة توقّف محمية بكلمة مرور في حال عدم اسـتخدام الجهاز (Session Timeout) لمدة 5 دقائق.
- 1-14 يجب إدارة أجهزة المسـتخدمين والأجهزة المحمولة مركزياً من خلال خادم الدليل النشط (Active Directory) الخاص بنطاق **جمعية اعتدال** أو نظام إداري مركزي.
- 1-15 يجب ضبط إعدادات أجهزة المسـتخدمين والأجهـزة المحمولة بإدارة الوحدات التنظيمية المناسـبة (Domain Controller) لتطبيـق السياسـات الملائمة وتثبيت الإعـدادات البرمجية اللازمة.
- 1-16 يجـب تنفيذ سياسـات النطاق المناسـبة (Group Policy) في **جمعيـة اعتدال** وتطبيقها في جميع أجهزة المستخدمين والأجهزة المحمولة لضمان الالتزام بالضوابط التنظيمية والأمنية.

2. متطلبات الأمن السيبراني لأمن أجهزة المستخدمين

- 2-1 يجـب تخصيص أجهـزة المسـتخدمين للفريق التـقني ذي الصلاحيات الهامـة، وأن تكون معزولة في شـبكة خاصـة لإدارة الأنظمة (Management Network) ولا ترتبط بأي شـبكة أو خدمة أخرى.
- 2-2 يجب ضبط إعدادات أجهزة المسـتخدمين الهامة والحساسة والتي لها صلاحيات متقدمة لإرسال السجلات إلى نظام تسجيل ومراقبة مركزي وفقاً لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني، مع عدم إمكانية إيقافه عن طريق المستخدم.
- 2-3 يجب تأمين أجهزة المستخدمين مادياً داخل مبنى **جمعية اعتدال.**

3. متطلبات الأمن السيبراني لأمن الأجهزة المحمولة

- 3-1 يجب منع وصول الأجهزة المحمولة إلى الأنظمة الحساسة إلا لفترة مؤقتة فقط، وذلك بعد إجراء تقييم المخاطر وأخذ الموافقات اللازمة من إدارة تقنية المعلومات.(CSCC-2-5-1-1)
- 3-2 يجب تشفير أقراص الأجهزة المحمولة التي تملك صلاحية الوصول للأنظمة الحساسة تشفيراً كاملاً (Full Disk Encryption). (CSCC-2-5-1-2)

4. متطلبات الأمن السيبراني لأمن الأجهزة الشخصية (BYOD)

- 4-1 يجب إدارة الأجهزة المحمولة مركزياً باستخدام نظام إدارة الأجهزة المحمولة (Mobile Device Management "MDM").
- 4-2 يجب فصل وتشفير البيانات والمعلومات الخاصة **بـجمعية اعتدال** المخزنة على الأجهزة الشخصية للعاملين (BYOD).
- 5- متطلبات أخرى
- 5-1 إجراء نسخ احتياطي دوري للبيانات المخزّنة على أجهزة المستخدمين والأجهزة المحمولة، وذلك وفقاً لسياسة النسخ الاحتياطية المعتمدة في **جمعية اعتدال.**
- 5-2 تُحذَف بيانات **جمعية اعتدال** المُخزّنة على الأجهزة المحمولة والأجهزة الشخصية (BYOD) في الحالات التالية:
  - فقدان الجهاز المحمول أو سرقته.
  - انتهاء أو إنهاء العلاقة الوظيفية بين المستخدم وجمعية اعتدال.
- 5-3 يجب نشر الوعي الأمني للعاملين حول آلية استخدام الأجهزة ومسؤولياتهم تجاهها وفقاً لسياسة الاستخدام المقبول المعتمدة في **جمعية اعتدال** وإجراء جلسات توعية خاصة بالمستخدمين ذوي الصلاحيات الهامة والحساسة.
- 5-4 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لحماية أجهزة المستخدمين والأجهزة المحمولة.
- 5-5 يجب مراجعة سياسة أمن أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية سنوياً، وتوثيق التغييرات واعتمادها.

الأدوار والمسؤوليات

1. راعي ومالك وثيقة السياسة: مدير إدارة تقنية المعلومات.
2. مراجعة السياسة وتحديثها: إدارة تقنية المعلومات.
3. تنفيذ السياسة وتطبيقها: إدارة تقنية المعلومات.

الالتزام بالسياسة

1. يجب على مدير إدارة تقنية المعلومات ضمان التزام **جمعية اعتدال** بهذه السياسة دورياً.
2. يجب على إدارة تقنية المعلومات في **جمعية اعتدال** الالتزام بهذه السياسة.
3. قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في **جمعية اعتدال.**

ثالثاً : سياسة إدارة هويات الدخول والصلاحيات

الأهداف

- الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بإدارة هويات الدخول والصلاحيات على الأصول المعلوماتية والتقنية الخاصة **بجمعية اعتدال** لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية، وذلك من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم 2-2-1 من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

- تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة **بجمعية اعتدال**، وتنطبق على جميع العاملين في جمعية اعتدال.

بنود السياسة

1- إدارة هويات الدخول والصلاحيات (Identity and Access Management)

1-1 إدارة الصلاحيات

- 1-1-1 توثيق واعتماد إجراء لإدارة الوصول يوضح آلية منح صلاحيات الوصول للأصول المعلوماتية والتقنية وتعديلها وإلغائها في **جمعية اعتدال**، ومراقبة هذه الآلية والتأكد من تطبيقها.
- 1-1-2 إنشاء هويات المستخدمين (User Identities) وفقاً للمتطلبات التشريعية والتنظيمية الخاصة بجمعية اعتدال.
- 1-1-3 التحقق من هوية المستخدم (Authentication) والتحقق من صحتها قبل منح المستخدم صلاحية الوصول إلى الأصول المعلوماتية والتقنية.
- 1-1-4 توثيق واعتماد مصفوفة (Matrix) لإدارة تصاريح وصلاحيات المستخدمين (Authorization) بناءً على مبادئ التحكم بالدخول والصلاحيات التالية:
  - 1-1-4-1مبدأ الحاجة إلى المعرفة والاستخدام (Need-to-Know and Need-to-Use).
  - 1-1-4-2مبدأ فصل المهام (Segregation of Duties).
  - 1-1-4-3مبدأ الحد الأدنى من الصلاحيات والامتيازات (Least Privilege).
- 1-1-5 تطبيق ضوابط التحقّق والصلاحيات على جميع الأصول التقنية والمعلوماتية في جمعية اعتدال من خلال نظام مركزي آلي للتحكّم في الوصول، مثل بروتوكول النفاذ إلى الدليل البسيط ("Lightweight Directory Access Protocol "LDAP).
- 1-1-6 منع استخدام الحسابات المشتركة (Generic User) للوصول إلى الأصول المعلوماتية والتقنية الخاصة **بجمعية اعتدال**

- 1-1-7 ضبط إعدادات الأنظمة ليتم إغلاقها تلقائياً بعد فترة زمنية محدّدة (Session Timeout)، (يوصى ألا تتجاوز الفترة 15 دقيقة).
- 1-1-8 تعطيل حسابات المستخدمين غير المستخدمة خلال فترة زمنية محدّدة (يوصى ألا تتجاوز الفترة 90 يوماً.)
- 1-1-9 ضبط إعدادات جميع أنظمة إدارة الهويات والوصول لإرسال السجلات إلى نظام تسجيل ومراقبة مركزي وفقاً لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني.
- 1-1-10 عدم منح المستخدمين صلاحيات الوصول أو التعامل المباشر مع قواعد البيانات للأنظمة الحساسة، حيث يكون ذلك من خلال التطبيقات فقط، ويستثنى من ذلك مشرفي قواعد البيانات (Database Administrators). [CSCC-2-2-1-7]
- 1-1-11 توثيق واعتماد إجراءات واضحة للتعامل مع حسابات الخدمات (Service Account) والتأكد من إدارتها بشكل آمن ما بين التطبيقات والأنظمة، وتعطيل الدخول البشري التفاعلي (InteractiveLogin) من خلالها. (CSCC-2-2-1-7)

2-1 منح حق الدخول

1-2-1 متطلبات حق الدخول لحسابات المستخدمين

- 1-2-1-1 منح صلاحية الدخول بناءً على طلب المستخدم من خلال نموذج أو عن طريق النظام المعتمد من قبل مديره المباشر ومالك النظام (System Owner) يُحدّد فيه اسم النظام ونوع الطلب والصلاحية ومدتها (في حال كانت صلاحية الدخول مؤقتة).
- 1-2-1-2 منح المستخدم حق الوصول إلى الأصول المعلوماتية والتقنية الخاصة بجمعية اعتدال بما يتوافق مع الأدوار والمسؤوليات الخاصة به.
- 1-2-1-3 اتباع آلية موحدة لإنشاء هويات المستخدمين بطريقة تتيح تتبع النشاطات التي يتم أداؤها باستخدام "هوية المستخدم" (User ID) وربطها مع المستخدم.
- 1-2-1-4 تعطيل إمكانية تسجيل دخول المستخدم من أجهزة حاسبات متعدّدة في نفس الوقت (Concurrent Logins).

2-2-1 متطلبات حق الوصول للحسابات الهامة والحسّاسة

الإضافة إلى الضوابط المذكورة في قسم متطلبات حق الوصول لحسابات المستخدمين، يجب أن تُطبّق الضوابط المُوضّحة أدناه على الحسابات ذات الصلاحيات الهامة والحسّاسة:

- 1-2-2-1 تعيين حق وصول مستخدم فردي للمستخدمين الذين يطلبون الصلاحيات الهامة والحسّاسة ومنحهم هذا الحق بناءً على مهامهم الوظيفية، مع الأخذ بالاعتبار مبدأ فصل المهام.
- 1-2-2-2 يجب تفعيل سجل كلمة المرور (Password History) لتتبع عدد كلمات المرور التي تم تغييرها.
- 1-2-2-3 تغيير أسماء الحسابات الافتراضية، وخصوصاً الحسابات الحاصلة على صلاحيات هامة وحسّاسة مثل "الحساب الرئيسي" وحساب "مدير النظام" وحساب "مُعرّف النظام الفريد"

- 1-2-2-4 منع اســتخدام الحســابات ذات الصلاحيات الهامة والحسّاســة في العمليات التشغيلية اليومية.
- 1-2-2-5 التحقّق من حســابات المســتخدمين ذات الصلاحيات الهامة والحسّاسة على الأصول التقنيــة والمعلوماتيــة مــن خلال آليــة التحقّق مــن الهوية متعــدد العنــاصر (Multi-Factor Authentication "MFA") باستخدام طريقتين على الأقل من الطرق التالية:
  - المعرفة (شيء يعرفه المستخدم "مثل كلمة المرور").
  - الحيــازة (شيء يملكــه المســتخدم فقط "مثل برنامج أو جهاز توليد أرقام عشــوائية أو الرســائل القصيرة المؤقتة لتسجيل الدخول .
  - الملازمة (صفة أو سمة حيوية متعلقة بالمستخدم نفسه فقط "مثل بصة الإصبع").
- 1-2-2-6 يجب أن يتطلب الوصول إلى الأنظمة الحساســة والأنظمة المســتخدمة لإدارة الأنظمة الحساسة ومتابعتها استخدام التحقق من الهوية متعدد العناصر (MFA) لجميع المستخدمين.

1-2-3 الدخول عن بُعد إلى شبكة جمعية اعتدال

- 1-2-3-1 منــح صلاحيــة الدخول عن بعد للأصــول المعلوماتية والتقنية بعــد الحصول على إذن مسبق من إدارة تقنية المعلومات وتقييد الدخول باستخدام التحقق من الهوية متعدد العناصر (MFA).
- 1-2-3-2 حفظ ســجلات الأحداث المتعلقة بجميع جلســات الدخول عن بُعد الخاصة ومراقبتها حسب حساسية الأصول المعلوماتية والتقنية.

3-1 إلغاء وتغيير حق الوصول

- 1-3-1 يجـب على الإدارة المعنيـة تبليـغ إدارة تقنية المعلومات لاتخاذ الإجـراء اللازم عند انتقال المسـتخدم أو تغيير مهامـه أو إنهاء/انتهاء العلاقة الوظيفية بين المسـتخدم **وجمعية اعتدال.** وتقوم إدارة تقنية المعلومات بإيقاف أو تعديل صلاحيات الدخول الخاصة بالمسـتخدم بناءً على مهامه الوظيفية الجديدة.
- 2-3-1 في حـال تـم إيقـاف صلاحيـات المسـتخدم، يمنـع حـذف سـجلات الأحـداث الخاصة بالمستخدم ويتم حفظها وفقاً لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني.

2- مراجعة هويات الدخول والصلاحيات

- 2-1 مراجعة هويات الدخول (User IDs) والتحقق من صلاحية الوصول إلى الأصول المعلوماتية والتقنية وفقاً للمهام الوظيفية للمستخدم بناءً على مبادئ التحكم بالدخول والصلاحيات دورياً، ومراجعة هويات الدخول على الأنظمة الحساسة مرة واحدة كل ثلاثة أشهر على الأقل.
- 2-2 مراجعـة الصلاحيات الخاصة (User Profile) بالأصول المعلوماتية والتقنية بناءً على مبادئ التحكـم بالدخـول والصلاحيات دورياً، ومراجعـة الصلاحيات الخاصة بالأنظمة الحساسـة مرة واحدة سنوياً على الأقل.
- 2-3 يجب تسجيل وتوثيق جميع محاولات الوصول الفاشلة والناجحة ومراجعتها دورياً.

3- إدارة كلمات المرور

- 3-1 تطبيق سياسة آمنة لكلمة المرور ذات معايير عالية لجميع الحسابات **داخل جمعية اعتدال،** ويتضمّن الجدول أدناه أمثلة على ضوابط كلمات المرور لكل مستخدم:

ضوابط كلمات المرور	جميع المستخدمين (All Users)	حسابات المستخدمين ذات الصلاحيات الهامة والحسّاسة (Privileged Users)	حسابات الخدمات (Service Account)
الحـدّ الأدنى لعدد أحـرف كلمة المرور	8 أحـرف أو أرقام أو رموز	12 حرفـاً أو رقمـاً أو رمزاً	8 أحـرف أو أرقام أو رموز
سجل كلمة المرور	تذكّر 5 كلمات مرور	تذكّر 5 كلمات مرور	تذكّر 5 كلمات مرور
الحد الأعلى لعمر كلمة المرور	45 يوماً	45 يوماً	45 يوماً
مدى تعقيد كلمة المرور	مُفعّل	مُفعّل	مُفعّل
مثال على تعقيد كلمة المرور	D_dyW5$_	R@rS%7qY#b!u	r?M4d5V=
حد إغلاق الحساب	5 محاولات غير صحيحة لتسجيل الدخول	5 محاولات غير صحيحة لتسجيل الدخول	لا توجد محاولات

ضوابط كلمات المرور	جميع المستخدمين (All Users)	حسابات المستخدمين ذات الصلاحيات الهامة والحساسة (Privileged Users)	حسابات الخدمات (Service Account)
إعادة ضبط عداد إغلاق الحساب بعد مرور فترة معينة	8 أحـرف أو أرقام أو رموز	12 حرفـاً أو رقمـاً أو رمزاً	8 أحـرف أو أرقام أو رموز
استخـــــدام التحقـق متعـدد العناصر	مُفعـل على الدخول عن بعد فقط	مُفعل	غير مُفعل

3-2 معايير كلمات المرور

- 3-2-1 يجب أن تتضمّن كلمة المرور (8) أحرف على الأقل.
- 3-2-2 يجـب أن تكون كلمة المـرور معقّـدة (Complex Password) وتتضمّن ثلاثة رموز من الرموز التالية على الأقل:
- 3-2-1 أحرف كبيرة (Upper Case Letters).
- 3-2-2 أحرف صغيرة (Lower Case Letters).
- 3-2-3 أرقام (1235).
- 3-2-4 رموز خاصّة (#%*@).
- 3-2-3 يجب إشـعار المستخدمين قبل انتهاء صلاحية كلمة المرور لتذكيرهم بتغيير كلمة المرور قبل انتهاء الصلاحية.
- 3-2-4 يجـب ضبط إعدادات كافة الأصول المعلوماتية والتقنية لطلب تغيير كلمة المرور المؤقتة عند تسجيل المستخدم الدخول لأول مرة.
- 3-2-5 يجـب تغيير جميـع كلمات المرور الافتراضيـة لجميع الأصول المعلوماتيـة والتقنية قبل تثبيتها في بيئة الإنتاج.
- 3-2-6 يجـب تغيير كلمـات مرور السلاسـل النصيـة (Community String) الافتراضية (مثل: «Public» و«Private» و«System») الخاصة ببروتوكول إدارة الشبكة البسيط (SNMP)، ويجب أن تكون مختلفة عن كلمات المرور المستخدمة لتسجيل الدخول في الأصول التقنية المعنية.

3-3 حماية كلمات المرور

- 3-3-1 يجب تشفير جميع كلمات المرور للأصول المعلوماتية والتقنية الخاصة بـجمعية اعتدال بصيغة غير قابلة للقراءة أثناء إدخالها ونقلها وتخزينها وذلك وفقاً لسياسة التشفير.
- 3-3-2 يجب إخفاء (Mask) كلمة المرور عند إدخالها على الشاشة.
- 3-3-3 يجـب تعطيـل خاصية "تذكّـر كلمـة المـرور" (Remember Password) على الأنظمة والتطبيقات الخاصة بجمعية اعتدال
- 3-3-4 منع استخدام الكلمات المعروفة (Dictionary) في كلمة المرور كما هي.

- 3-3-5 يجب تسليم كلمة المرور الخاصة بالمستخدم بطريقة آمنة وموثوقة.
- 3-3-6 إذا طلب المستخدم إعادة تعيين كلمة المرور عن طريق الهاتف أو الإنترنت أو أي وسيلة أخرى، فلا بد من التحقّق من هوية المستخدم قبل إعادة تعيين كلمة المرور.
- 3-3-7 يجب حماية كلمات المرور الخاصة بحسابات الخدمة والحسابات ذات الصلاحيات الهامة والحسّاسة وتخزينها بشكل آمن في موقع مناسب (داخل مغلف مختوم في خزنة) أو استخدام التقنيات الخاصة بحفظ وإدارة الصلاحيات الهامة والحسّاسة (Privilege Access Management Solution).

4- متطلبات أخرى

- 4-1 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لإدارة هويات الدخول والصلاحيات.
- 4-2 يجب مراجعة تطبيق متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات دورياً.
- 4-3 يجب مراجعة هذه السياسة سنوياً على الأقل، أو في حال حدوث تغييرات في المتطلبات التشريعية أو التنظيمية أو المعايير ذات العلاقة.

الأدوار والمسؤوليات

1. راعي ومالك وثيقة السياسة: مدير إدارة تقنية المعلومات.
2. مراجعة السياسة وتحديثها: إدارة تقنية المعلومات.
3. تنفيذ السياسة وتطبيقها: إدارة تقنية المعلومات وإدارة الخدمات المشتركة

الالتزام بالسياسة

1. يجب على مدير إدارة تقنية المعلومات ضمان التزام **جمعية اعتدال** بهذه السياسة دورياً.
2. يجب على كافة العاملين في **جمعية اعتدال** الالتزام بهذه السياسة.
3. قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في **جمعية اعتدال.**

رابعاً : سياسة الاستخدام المقبول للأصول

الأهداف

الغـرض مـن هذه السياسـة هو توفير متطلبـات الأمن السـيبراني؛ لتقليـل المخاطر السـيبرانية، المتعلقة باستخدام **أنظمة جمعية اعتدال** وأصولها، وحمايتها من التهديدات الداخلية والخارجية، والعناية بالأهداف الأساسية للحماية؛ وهي المحافظة على سرية المعلومة، وسلامتها، وتوافرها.
وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم 2-1-3 من الضوابط الأساسـية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسـة جميـع الأصول المعلوماتية والتقنية الخاصة **بـجمعية اعتـدال** وتنطبق على جميع العاملين في **جمعية اعتدال.**

بنود السياسة

1. البنود العامة

- 1-1 يجـب التعامـل مع المعلومات حسـب التصنيـف المحدد، وبما يتوافق مع سياسـة تصنيف البيانات وسياسـة حماية البيانات والمعلومات الخاصة **بـجمعية اعتدال** بشـكل يضمن حماية سرية المعلومات وسلامتها وتوافرها.
- 1-2 يحظر انتهاك حقوق أي شخص، أو شركة محمية بحقوق النشر، أو براءة الاختراع، أو أي ملكية فكرية أخرى، أو قوانين أو لوائح مماثلة؛ بما في ذلك، على سـبيل المثال لا الحصر، تثبيت برامج غير مصرح بها أو غير قانونية.
- 1-3 يجب عدم ترك المطبوعات على الطابعة المشتركة دون رقابة.
- 1-4 يجب حفظ وسائط التخزين الخارجية بشكل آمن وملائم، مثل التأكد من ضبط درجة الحرارة بدرجة معينة، وحفظها في مكان معزول وآمن.
- 1-5 يمنع اسـتخدام كلمة المرور الخاصة بمسـتخدمين آخرين، بما في ذلك كلمة المرور الخاصة بمدير المستخدم أو مرؤوسيه.
- 1-6 يجب الالتزام بسياسة المكتب الآمن والنظيف، والتأكد من خلو سطح المكتب، وكذلك شاشة العرض من المعلومات المصنفة.
- 1-7 يمنـع الإفصـاح عن أي معلومات تخـص **جمعية اعتدال** ، بما في ذلـك المعلومات المتعلقة بالأنظمة والشبكات لأي جهة أو طرف غير مصرح له سواءً كان ذلك داخلياً أو خارجياً.
- 1-8 يُمنع نشر معلومات تخص **جمعية اعتدال** عبر وسـائل الإعلام، وشبكات التواصل الاجتماعي دون تصريح مسبق.
- 1-9 يُمنع اسـتخدام **أنظمة جمعية اعتدال** وأصولها بغرض تحقيق منفعة وأعمال شـخصية، أو تحقيق أي غرض لا يتعلق بنشاط وأعمال **جمعية اعتدال.**

- 1-10 يُمنع ربط الأجهزة الشخصية بالشبكات، والأنظمة الخاصة **بـجمعية اعتدال** دون الحصول على تصريح مسبق، وبما يتوافق مع سياسة أمن الأجهزة المحمولة (BYOD).
- 1-11 يُمنع القيام بأي أنشطة تهدف إلى تجاوز أنظمة الحماية الخاصة **بجمعية اعتدال**، بما في ذلك برامـج مكافحة الفيروسـات، وجدار الحمايـة، والبرمجيـات الضارة دون الحصـول على تصريح مسبق، وبما يتوافق مع الإجراءات المعتمدة لدى تراحم الشرقية.
- 1-12 تحتفظ إدارة تقنية المعلومات بحقها في مراقبة الأنظمة والشـبكات والحسـابات الشخصية المتعلقة بالعمل، ومراجعتها دورياً لمراقبة الالتزام بسياسات الأمن السيبراني ومعاييره.
- 1-13 يُمنع اسـتضافة أشـخاص غير مصرح لهم بالدخول للأماكن الحساسة دون الحصول على تصريح مسبق.
- 1-14 يجب ارتداء البطاقة التعريفية في جميع مرافق **جمعية اعتدال.**
- 1-15 يجب تبليغ إدارة تقنية المعلومات في حال فقدان المعلومات أو سرقتها أو تسريبها.

2. حماية أجهزة الحاسب الآلي

- 2-1 يمنع اسـتخدام وسـائط التخزين الخارجية دون الحصول على تصريح مسبق من إدارة تقنية المعلومات.
- 2-2 يُمنع القيام بأي نشاط من شأنه التأثير على كفاءة الأنظمة والأصول وسلامتها دون الحصول على إذن مسـبق من إدارة تقنية المعلومات ، بما في ذلك الأنشـطة التي تُمكّن المسـتخدم من الحصول على صلاحيات وامتيازات أعلى.
- 2-3 يجب تأمين الجهاز قبل مغادرة المكتب وذلك بقفل الشاشة، أو تسجيل الخروج (Sign out or Lock)، سواء كانت المغادرة لفترة قصيرة أو عند انتهاء ساعات العمل.
- 2-4 يُمنـع تـرك أي معلومات مصنفة في أماكن يسـهل الوصول إليهـا، أو الاطلاع عليها من قبل أشخاص غير مصرح لهم.
- 2-5 يُمنع تثبيت أدوات خارجية على جهاز الحاسـب الآلي دون الحصول على إذن مسبق من إدارة تقنية المعلومات .
- 2-6 يجـب تبليـغ إدارة تقنية المعلومات عند الاشـتباه بأي نشـاط قد يتسـبب بضرر على أجهزة الحاسب الآلي الخاصة **بـ جمعية اعتدال أو أصولها.**

3. الاستخدام المقبول للإنترنت والبرمجيات

- 3-1 يجب إبلاغ إدارة تقنية المعلومات في حال وجود مواقع مشبوهة ينبغي حجبها؛ أو العكس.
- 3-2 يجب ضمان عدم انتهاك حقوق الملكية الفكرية أثناء تنزيل معلومات أو مستندات لأغراض العمل.
- 3-3 يُمنع استخدام البرمجيات غير المرخصة أو غيرها من الممتلكات الفكرية.
- 3-4 يجب استخدام متصفح آمن ومصرح به للوصول إلى الشبكة الداخلية أو شبكة الإنترنت.
- 3-5 يُمنع اسـتخدام التقنيات التي تسـمح بتجاوز الوسـيط (Proxy) أو جدار الحماية (Firewall) للوصول إلى شبكة الإنترنت.

- 3-6 يُمنـع تنزيـل البرمجيـات والأدوات أو تثبيتها على أصول **جمعية اعتـدال** دون الحصول على تصريح مسبق من إدارة تقنية المعلومات .
- 3-7 يُمنع اسـتخدام شـبكة الإنترنت في غير أغراض العمل، بما في ذلك تنزيل الوسـائط والملفات واستخدام برمجيات مشاركة الملفات.
- 3-8 يجب تبليغ إدارة تقنية المعلومات عند الاشـتباه بوجود مخاطر سـيبرانية، كما يجب التعامل بحذر مع الرسائل الأمنية التي قد تظهر خلال تصفح شبكة الإنترنت أو الشبكات الداخلية.
- 3-9 يُمنـع إجـراء فحـص أمني لغـرض اكتشـاف الثغـرات الأمنية، ويشـمل ذلك إجـراء اختبار الاختراقات، أو مراقبة شـبكات تراحم الشرقية وأنظمتها، أو الشبكات والأنظمة الخاصة بالجهات الخارجية دون الحصول على تصريح مسبق من إدارة تقنية المعلومات .
- 3-10 يُمنع اسـتخدام مواقع مشـاركة الملفات دون الحصول على تصريح مسبق من إدارة تقنية المعلومات.
- 3-11 يُمنع زيارة المواقع المشبوهة بما في ذلك مواقع تعليم الاختراق.

4. الاستخدام المقبول للبريد الإلكتروني ونظام الاتصالات

- 4-1 يُمنع اسـتخدام البريد الإلـكتروني أو الهاتف أو الفاكس أو الفاكـس الإلكتروني في غير أغراض العمل، وبما يتوافق مع سياسات الأمن السيبراني ومعاييره.
- 4-2 يُمنع تداول رسائل تتضمن محتوى غير لائق أو غير مقبول، بما في ذلك الرسائل المتداولة مع الأطراف الداخلية والخارجية.
- 4-3 يجب استخدام تقنيات التشفير عند إرسال معلومات حساسة عن طريق البريد الإلكتروني أو أنظمة الاتصالات.
- 4-4 يجب عدم تسـجيل عنوان البريد الإلكتروني الخاص **بـجمعية اعتـدال** في أي موقع ليس له علاقة بالعمل.
- 4-5 يجب تبليغ إدارة تقنية المعلومات عند الاشـتباه بوجود رسائل بريد إلكتروني تتضمن محتوى قد يتسبب بأضرار لأنظمة **جمعية اعتدال أو أصولها.**
- 4-6 **تحتفظ جمعية اعتدال** بحقها في كشـف محتويات رسائل البريد الإلكتروني بعد الحصول على التصاريح اللازمة من صاحب الصلاحية وإدارة تقنية المعلومات وفقاً للإجراءات والتنظيمات ذات العلاقة.
- 4-7 يُمنع فتح رسائل البريد الإلكتروني والمرفقات المشبوهة أو غير المتوقعة حتى وإن كانت تبدو من مصادر موثوقة.

5. الاجتماعات المرئية والاتصالات القائمة على شبكة الإنترنت

- 5-1 يُمنع استخدام أدوات أو برمجيات غير مصرح بها لإجراء اتصالات أو عقد اجتماعات مرئية.
- 5-2 يُمنـع إجـراء اتصالات أو عقد اجتماعـات مرئية لا تتعلق بالعمـل دون الحصول على تصريح مسبق.

6. استخدام كلمات المرور

- 6-1 يجـب اختيـار كلمات مرور آمنـة، والمحافظة على كلمـات المرور الخاصـة **بأنظمة جمعية اعتدال** وأصولها. كما يجب اختيار كلمات مرور مختلفة عن كلمات مرور الحسـابات الشـخصية، مثل حسابات البريد الشخصي ومواقع التواصل الاجتماعي.
- 6-1 يُمنع مشاركة كلمة المرور عبر أي وسيلة كانت، بما في ذلك المراسلات الإلكترونية، والاتصالات الصوتية، والكتابة الورقية. كما يجب على جميع المستخدمين عدم الكشف عن كلمة المرور لأي طرف آخر بما في ذلك زملاء العمل وموظفو إدارة تقنية المعلومات.
- 6-2 يجب تغيير كلمة المرور، عند تزويدك بكلمة مرور جديدة من قبل مسؤول النظام.

الأدوار والمسؤوليات

1. راعي ومالك وثيقة السياسة: مدير إدارة تقنية المعلومات.
2. مراجعة السياسة وتحديثها: إدارة تقنية المعلومات.
3. تنفيذ السياسة وتطبيقها: إدارة تقنية المعلومات وجميع العاملين.

الالتزام بالسياسة

1. يجب على مدير إدارة تقنية المعلومات ضمان التزام **جمعية اعتدال** بهذه السياسة بشكل دوري.
2. يجب على جميع العاملين في **جمعية اعتدال** الالتزام بهذه السياسة.
3. قـد يُعرّض أي انتهاك لهذه السياسـة صاحب المخالفة إلى إجراء تأديبي؛ حسـب الإجـراءات المُتبعة في **جمعية اعتدال .**

خامساً : سياسة الأمن السيبراني ضمن استمرارية الأعمال

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير ضمن إدارة استمرارية الأعمال **لضمان استمرارية أعمال جمعية اعتدال وحمايتها** من المخاطر السيبرانية والتهديدات الداخلية والخارجية، ويتم ذلك من خلال التركيز على هدف التوافر وهو من الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم 3-1-1 من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) والضابط رقم 3-1-1 من ضوابط الأمن السيبراني للأنظمة الحساسة (CSCC-1:2019) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة إدارة استمرارية الأعمال الخاصة بالأمن السيبراني في **جمعية اعتدال** وتنطبق على جميع العاملين في **جمعية اعتدال.**

بنود السياسة

1. يجب التأكد من استمرارية الأنظمة والإجراءات المتعلقة بالأمن السيبراني في **جمعية اعتدال.**
2. يجب إجراء تقييم للمخاطر التي قد تؤثر **على استمرارية أعمال جمعية اعتدال.**
3. يجب معالجة نقاط الضعف لتجنب الحوادث التي قد تؤثر على استمرارية **أعمال جمعية اعتدال.**
4. يجب تحديد المتطلبات التشريعية والتنظيمية الخاصة باستمرارية الأعمال **لدى جمعية اعتدال.**
5. يجب وضع خطط الاستجابة لحوادث الأمن السيبراني التي قد تؤثر على استمرارية **أعمال جمعية اعتدال.**
6. يجب وضع خطط التعافي من الكوارث (Disaster Recovery Plan).
7. يجب إدراج الأنظمة الحساسة **لجمعية اعتدال** ضمن خطط التعافي من الكوارث.
8. يجب إنشاء مركز للتعافي من الكوارث للأنظمة الحساسة.
9. يجب إجراء اختبارات دورية للتأكد من فعالية خطط التعافي من الكوارث للأنظمة الحساسة **لجمعية اعتدال** مرة واحدة سنويًا على الأقل.
10. يجب إجراء اختبار دوري حي للتعافي من الكوارث (Live DR Test) للأنظمة الحساسة.
11. يجب تضمين حوادث الأمن السيبراني عالية الخطورة ضمن الأسباب الموجبة لتفعيل **خطة استمرارية الأعمال في جمعية اعتدال.**
12. يجب إجراء تحليل التأثير على الأعمال (Business Impact Analysis) لتحديد الأنظمة الحساسة في **جمعية اعتدال** ونسخها إلى موقع التعافي من الكوارث.
13. يجب تحديد متطلبات النسخ الدورية الخاصة بالأنظمة الحساسة **لجمعية اعتدال** إلى مركز التعافي.
14. يجب تضمين خطط استمرارية سلاسل التوريد والإمداد **ضمن خطط استمرارية أعمال جمعية اعتدال.**

15. يجب تضمين طرق التواصل الخاصة بفريق الأمن السيبراني في **جمعية اعتدال** سواءً الداخلية أو الخارجية وتوثيقها.
16. يجب تحديد الأدوار والمسؤوليات للأطراف ذات العلاقة باستمرارية الأعمال **في جمعية اعتدال.**
17. يجب وضع خطط تنفيذ ومتابعة المسؤوليات والأعمال الخاصة بالأمن السيبراني خلال الكوارث ولحين عودة الأوضاع لطبيعتها.
18. يجب إدارة هويات الدخول والصلاحيات على جميع الأنظمة والبيانات المستضافة في موقع التعافي من الكوارث **الخاص بجمعية اعتدال** لضمان عدم الوصول إليها من قبل الأشخاص غير المصرح لهم.
19. يجب تضمين متطلبات خطط التعافي من الكوارث في عقود واتفاقيات جمعية اعتدال مع الأطراف الخارجية ومقدمي الخدمات السحابية.
20. يجب ضمان تطبيق الضوابط الأساسية للأمن السيبراني (ECC-1:2018) في بيئة مركز التعافي من الكوارث **التابع لـ جمعية اعتدال** مثل: الأمن المادي، أمن الشبكة والبنية التحتية، أمن البيانات والمعلومات، التشفير، إلخ.
21. يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لمتطلبات الأمن السيبراني الخاصة باستمرارية أعمال الأمن السيبراني.

الأدوار والمسؤوليات

1. راعي ومالك وثيقة السياسة: مدير إدارة تقنية المعلومات.
2. مراجعة السياسة وتحديثها: إدارة تقنية المعلومات.
3. تنفيذ السياسة وتطبيقها: إدارة تقنية المعلومات.

الالتزام بالسياسة

1. يجب على مدير إدارة تقنية المعلومات ضمان التزام **جمعية اعتدال** بهذه السياسة بشكل دوري.
2. يجب على جميع العاملين في **جمعية اعتدال** الالتزام بهذه السياسة.
3. قد يُعرِض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في **جمعية اعتدال .**

اعتماد مجلس الإدارة

تـم اعتماد **سياســات وحدة تقنيــة المعلومات** بجمعية اعتـدال للتكافل والاسـتدامة في اجتماع مجلس الإدارة رقم 2 / 6 2026، المنعقد بتاريخ 28 / 01 / 1448هـ، الموافق 13 / 07 / 2026م.

اعتدال
للتكافل والاستدامة
ETEDAL SOLIDARITY & SUSTAINABILITY

+966 92 003 2542
info@etedal.org.sa
Kingdom of Saudi Arabia / Dammam
المملكة العربية السعودية / الدمام
etedal_sa