إشراق
الجمعية السعودية لاضطراب فـرط الحركة وتشتت الانتبـاه
SAUDI ADHD SOCIETY

مسجلة بالمركز الوطني لتنمية القطاع غير الربحي برقم (474)

دليل سياسة تقنية وأمن المعلومات

بيان التعديل			
رقم التعديل	التاريخ	رقم الصفحة	ملخص التعديل

إعداد	مراجعة	اعتماد
الأستاذة نبال بنت عبدالعزيز الهذيل مدير الجودة والتميز المؤسسي	الأستاذة نوال بنت محمد الشريف المدير التنفيذي	سمو الأميرة نوف بنت محمد بن عبدالله رئيس مجلس الإدارة

دليل سياسة تقنية وأمن المعلومات

أولاً: سياسة الاستخدام المقبول لتقنية المعلومات

مادة (1): الغرض من السياسة

تهدف هذه السياسة إلى وضع الأطر والضوابط والقواعد العامة التي تنظم الاستخدام المقبول للأجهزة والبرامج والأنظمة التقنية التابعة لجمعية إشراق، بما يضمن الاستخدام الآمن والمهني لموارد تقنية المعلومات، ويحقق حماية متوازنة لكل من الجمعية ومنسوبيها.

وقد وُضعت هذه القواعد بهدف الحد من المخاطر التقنية والأمنية والقانونية التي قد تنشأ نتيجة سوء الاستخدام أو الإهمال، والتي قد تشمل – على سبيل المثال لا الحصر – انتشار الفيروسات، اختراق الشبكات أو الأنظمة، تسريب البيانات، أو التعرض للمساءلة القانونية.

مادة (2): نطاق تطبيق السياسة

أولاً: الفئات المشمولة

تسري أحكام هذه السياسة على جميع منسوبي جمعية إشراق، ويشمل ذلك:

- الموظفين بدوام كامل.
- الموظفين بدوام جزئي.
- المتطوعين.
- المتعاقدين أو المستشارين الذين لديهم صلاحية استخدام أجهزة أو أنظمة الجمعية.

ثانياً: الاستثناءات

يُستثنى من بعض القيود الواردة في هذه السياسة منسوبو إدارة تقنية المعلومات، وذلك في حدود مهامهم الوظيفية، ويشمل ذلك:

- تنصيب البرامج على أجهزة الجمعية.
- إجراء أعمال الصيانة الفنية أو نقل الأجهزة إلى مراكز الصيانة الخارجية.
- تعديل إعدادات الشبكة أو فصل وتوصيل كيابل الشبكة والتوصيلات التقنية الأخرى.

ثالثاً: نطاق التغطية

تشمل هذه السياسة جميع مكونات تقنية المعلومات في الجمعية، وعلى وجه الخصوص:

- أجهزة الحاسب الآلي بجميع أنواعها.
- الأجهزة الإلكترونية الأخرى وملحقاتها.
- البرامج والأنظمة.
- أنظمة التشغيل المختلفة.
- وسائط تخزين البيانات.
- حسابات المستخدمين على الشبكات والأنظمة السحابية.
- استخدام الإنترنت.
- حسابات الاتصال الآمن.(VPN)

مادة (3): عدم الامتثال

يُعد عدم الالتزام بالقواعد والتعليمات الواردة في هذه السياسة مخالفة إدارية، ويترتب عليها تطبيق الجزاءات المنصوص عليها في لائحة تنظيم العمل المعتمدة في جمعية إشراق، مع احتفاظ الجمعية بحقها في اتخاذ الإجراءات القانونية والقضائية اللازمة للمطالبة بالتعويض عن أي أضرار ناتجة عن تلك المخالفات.

مادة (4): حقوق الملكية والاستخدام

تُعد جميع الأجهزة والبيانات والمعلومات والملفات الإلكترونية التي يتم إنتاجها أو تداولها أو تخزينها باستخدام موارد تقنية المعلومات التابعة للجمعية أصولًا مملوكة ملكية كاملة لجمعية إشراق.

ولا يجوز التصرف في هذه الأصول، سواء بالحذف أو النقل أو النسخ أو المشاركة، إلا في حدود الصلاحيات المعتمدة للمستخدم أو بموافقة رسمية صريحة من الجمعية.

مادة (5): حفظ البيانات والملفات

أولاً: آلية التخزين

تلتزم الجمعية بتنظيم حفظ البيانات وفق الآتي:

1. تُخزن البيانات الخام في الأنظمة الإلكترونية التي تديرها الجمعية، بما في ذلك – على سبيل المثال لا الحصر – بيانات المستفيدين، بيانات الداعمين، بيانات طلبات الخدمات، والبيانات المالية والفواتير.
2. تُخزن الملفات الإلكترونية إما في:
   - OneDrive الخاص بالموظف ضمن بيئة Microsoft 365.
   - الفرق الإدارية المعتمدة على Microsoft Teams.

ثانياً: محظورات التخزين

يُحظر تخزين ملفات العمل على:

- وسائط تخزين شخصية.
- خدمات سحابية شخصية مثل Google Drive أو غيرها.
- أجهزة الحاسب خارج المواقع المحددة للتخزين (مثل سطح المكتب) ما لم تكن مزامنة رسميًا.

مادة (6): صلاحيات الدخول على البيانات ومشاركتها

1. تُدار صلاحيات الدخول إلى البيانات والأنظمة وفق قائمة صلاحيات معتمدة.(Access Control List)
2. يتم التنسيق بشأن طلب أو تعديل صلاحيات الدخول من خلال إدارة تقنية المعلومات فقط.

مادة (7): الصيانة والصيانة الوقائية

1. تُجرى أعمال الصيانة الدورية للأجهزة والأنظمة في نهاية كل عام ميلادي، وتُنفذ الصيانة الطارئة عبر نظام الدعم الفني.
2. يختص بأعمال الصيانة أخصائيو الدعم الفني والشبكات، ويُمنع على أي موظف إجراء صيانة ذاتية أو الاستعانة بجهات خارجية.
3. يجوز لإدارة تقنية المعلومات الاستعانة بفنيين خارجيين تحت إشرافها المباشر عند الحاجة.

مادة (8): التوجيهات الأمنية العامة

يلتزم المستخدم بما يلي:

1. الاطلاع فقط على البيانات اللازمة لأداء مهامه.
2. حماية جميع الأجهزة بكلمات مرور، بما في ذلك الأجهزة في الأماكن العامة.
3. تفعيل شاشة توقف تلقائية بعد 5 دقائق تتطلب كلمة مرور.
4. عدم تمثيل الجمعية في وسائل التواصل الاجتماعي إلا بتكليف رسمي.
5. منع تخزين البيانات على وسائط قابلة للإزالة، والاستعاضة عنها بالتخزين السحابي المعتمد.

مادة (9): الاستخدام غير المقبول

يُحظر بشكل قاطع:

- انتهاك حقوق الملكية الفكرية.
- الدخول غير المصرح به للأنظمة أو البيانات.
- إدخال برامج ضارة أو خبيثة.
- تجاوز أنظمة الحماية.
- استخدام أجهزة الجمعية لأغراض شخصية أو ترفيهية.
- مشاهدة محتوى غير لائق.
- إساءة استخدام اسم أو شعار الجمعية.
- تعطيل الشبكة أو الأجهزة.
- تسريب البيانات.
- أي تصرف يؤدي إلى الإضرار بأمن المعلومات أو استمرارية أعمال الجمعية.

مادة (10): كلمات المرور

أولاً: خصائص كلمات المرور

- ألا تقل عن 8 خانات.
- تحتوي على أحرف كبيرة وصغيرة ورموز.
- تُغيّر كل 90 يومًا.
- يُمنع إعادة استخدام آخر ثلاث كلمات مرور.

ثانياً: التنبيهات

- يُمنع تدوين كلمات المرور.
- يُمنع مشاركتها بأي وسيلة.
- يتحمل المستخدم المسؤولية الكاملة عن حسابه.

مادة (11): استخدام البريد الإلكتروني

يُعد البريد الإلكتروني الوسيلة الرسمية للتواصل، ويُستخدم حصريًا لأغراض العمل، ويُمنع:

- إرسال رسائل جماعية غير مصرح بها.
- إرسال طلبات تبرعات جماعية.
- إعادة توجيه رسائل حساسة دون مراعاة سريتها.

ويجوز للجمعية فحص البريد الإلكتروني عند الاشتباه بإساءة الاستخدام بعد موافقة الإدارة.

مادة (12): أمن البريد الإلكتروني والمرفقات

يلتزم المستخدم بالحذر من الرسائل المشبوهة، وعدم فتح المرفقات أو الروابط غير الموثوقة، والتواصل فورًا مع إدارة تقنية المعلومات عند الاشتباه.

ثانيًا: سياسة استخدام الأجهزة الشخصية في العمل

مادة (13): الغرض من السياسة

تهدف هذه السياسة إلى تنظيم استخدام الأجهزة الشخصية في تنفيذ أعمال الجمعية، وضمان حماية البيانات وأمن المعلومات.

مادة (14): نطاق التطبيق

تسري هذه السياسة على جميع الموظفين والمتطوعين والمتعاقدين دون استثناء.

مادة (15): الأجهزة المسموح باستخدامها

- الحواسيب المحمولة.
- الحواسيب المكتبية الشخصية.
- الهواتف الذكية.
- الأجهزة اللوحية.

مادة (16): تصنيف الأعمال

1. تُعد الأعمال المنفذة عبر حسابات أو شبكات الجمعية أعمالًا رسمية.
2. الأعمال الأخرى لا تتحمل الجمعية مسؤوليتها.

مادة (17): أمن الجهاز الشخصي

يلتزم المستخدم بـ:

- تأمين الجهاز بكلمة مرور.
- تثبيت برامج حماية.
- عدم استخدام أجهزة مخترقة أو مقرصنة.

مادة (18): الصيانة وإدارة الأجهزة

- التنسيق مع الدعم الفني قبل الصيانة.
- الالتزام بأنظمة إدارة الأجهزة عند تطبيقها.
- الإبلاغ عن فقدان الجهاز خلال 4 ساعات.

مادة (19): الاتصال بالشبكات

- الأجهزة الشخصية تتصل بشبكة الزوار فقط.
- الاتصال الخارجي يتم عبر VPN معتمد.

مادة (20): تراخيص البرامج

- استخدام البرامج المرخصة فقط.
- إزالة البرامج أو تسجيل الخروج منها عند انتهاء العلاقة الوظيفية.

ثالثًا: سياسة استخدام أنظمة الذكاء الاصطناعي

مادة (21): الغرض من السياسة

تهدف هذه السياسة إلى تنظيم استخدام أنظمة الذكاء الاصطناعي (AI) من قبل موظفي الجمعية، بما يضمن حماية خصوصية العملاء وسرية المعلومات، ويحافظ على الامتثال للأنظمة والتشريعات ذات العلاقة.

مادة (22): نطاق التطبيق

تسري هذه السياسة على جميع الموظفين والمتطوعين والمتعاقدين دون استثناء.

مادة (23): تعريفات

1. **الذكاء الاصطناعي (AI):** أي تقنية تعتمد على معالجة البيانات تلقائيًا باستخدام خوارزميات التعلم الآلي أو الشبكات العصبية أو أدوات تحليل ذكية.
2. **أدوات AI خارجية:** مثل ChatGPT ، Bard Google، Copilot، وغيرها من الأنظمة غير المملوكة للجمعية.
3. **معلومات حساسة:** أي معلومات تتعلق بالمتعاملين مع الجمعية من مستفيدين، أو متبرعين، أو متعاونين، أو متطوعين، أو العقود، أو المنتجات، أو الاستراتيجيات، أو البيانات المالية، أو البيانات الشخصية للموظفين، أو بيانات المساعدات المقدمة.

مادة (24): عدم الامتثال للسياسة

يُعد عدم الالتزام بالقواعد والتعليمات الواردة في هذه السياسة مخالفة إدارية، ويترتب عليها تطبيق الجزاءات المنصوص عليها في لائحة تنظيم العمل المعتمدة في جمعية إشراق، مع احتفاظ الجمعية بحقها في اتخاذ الإجراءات القانونية والقضائية اللازمة للمطالبة بالتعويض عن أي أضرار ناتجة عن تلك المخالفات.

مادة (25): المبادئ العامة

1. يسمح باستخدام أدوات الذكاء الاصطناعي فقط للأغراض المهنية المصرح بها.
2. يمنع إدخال أو مشاركة أي معلومات مصنفة على أنها "سرية" أو "خاصة" دون موافقة مسبقة.
3. يجب استخدام الأدوات المعتمدة فقط من قبل إدارة تقنية المعلومات.

مادة (26): المسموح وغير المسموح

يسمح باستخدام أنظمة الذكاء الاصطناعي في الحالات التالية، بشرط الالتزام بالضوابط الأمنية:

النشاط	مسموح/ غير مسموح	ملاحظات
توليد نصوص لأغراض تسويقية عامة	مسموح	بشرط مراجعتها قبل النشر
إعداد مسودات بريد إلكتروني داخلي	مسموح	بدون تضمين معلومات حساسة
تلخيص تقارير عامة غير سرية	مسموح	يجب مراجعة النتائج قبل استخدامها
تحليل بيانات المستفيدين والداعمين ومن في حكمهم	غير مسموح	فقط باستخدام أدوات داخلية معتمدة
تدريب أدوات الذكاء الاصطناعي باستخدام بيانات الجمعية	غير مسموح	يتطلب موافقة مكتوبة من الإدارة
استخدام حسابات شخصية للوصول إلى أدوات الذكاء الاصطناعي	غير مسموح	مرفوض باستخدام أجهزة الجمعية

مادة (27): الاستخدامات التالية غير مسموحة

1. إدخال أي من البيانات التالية في أدوات ذكاء اصطناعي خارجية:
   - بيانات المستفيدين
   - بيانات المتبرعين والتبرعات
   - بيانات المتعاونين والمتطوعين
   - بيانات المساعدات المقدمة
   - المعلومات المالية الداخلية
   - استراتيجيات الأعمال
   - أسماء أو سجلات الموظفين
2. استخدام أدوات AI لأغراض شخصية من خلال أجهزة الشركة أو الشبكة المؤسسية.
3. مشاركة نتائج الذكاء الاصطناعي مباشرة مع العملاء دون مراجعة أو تدقيق بشري من قبل مختص في الجمعية أو مدير الإدارة.

مادة (28): التزامات الموظفين

1. قراءة وفهم هذه السياسة قبل استخدام أي أداة ذكاء اصطناعي.
2. الإبلاغ عن أي استخدام مشبوه أو غير مصرح به.
3. الحصول على الموافقة اللازمة عند الحاجة إلى استخدام أدوات غير مدرجة في قائمة الأدوات المعتمدة.

اعتماد مجلس الإدارة

تم اعتماد دليل سياسة تقنية وأمن المعلومات في اجتماع مجلس الإدارة رقم (2026-2) المنعقد يوم السبت بتاريخ 2026/5/16م الموافق 1447/11/29هـ