- أي فرد أو جهة تعرف أو تشك أن أحد شركاء الجمعية أو من يعمل نيابة عنها قد أشترك في أعمال أو أنشطة تنتهك قواعد السلوك المهنية، يجب أن يفصح عما لديه عبر رابط تقديم الشكاوى في الموقع الجمعية ومن ثم الإبلاغ عن المخاوف لإدارة الجمعية.
- استقبال الشكاوى والإفصاح عن المخاوف يديرها فريق متخصص، حيث يمكن الحفاظ على سرية هويتك (بقدر ما يسمح به النظام).

المسؤوليات :

تطبق هذه السياسة ضمن أنشطة الجمعية وعلى جميع العاملين الذين يعملون تحت إدارة وإشراف الجمعية الاطلاع على الأنظمة المتعلقة بعملهم وعلى هذه السياسة والإلمام بها والتوقيع عليها، والالتزام بما ورد فيها من أحكام عند أداء واجباتهم ومسؤولياتهم الوظيفية , وعلى إدارة الموارد التنفيذية نشر الوعي بثقافة ومبادئ السلوك الوظيفي وأخلاقيات الوظيفة وتزويد جميع الإدارات والأقسام بنسخة منها.

سياسة الأمن السيبراني للموارد البشرية

الأهداف :

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لضمان التأكد من أن مخاطر ومتطلبات الأمن السيبراني المتعلقة بالعاملين (موظفين ومتعاقدين), في جمعية مديم الرقمية تعالج بفعالية قبل وأثناء وعند انتهاء/إنهاء عملهم.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-٩-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق :

تغطي هذه السياسة جميع الأنظمة الخاصة بـجمعية مديم الرقمية وتنطبق على جميع العاملين في جمعية مديم الرقمية.

بنود السياسة :

1. البنود العامة :

1-1 يجب تحديد متطلبات الأمن السيبراني المتعلقة بالعاملين.

2-1 يجب أن يشغل الوظائف ذات العلاقة بالأنظمة الحساسة في جمعية مديم الرقمية مواطنين ذو الكفاءة اللازمة.

3-1 يجب تنفيذ ضوابط الأمن السيبراني الخاصة بالموارد البشرية خلال دورة حياة عمل الموظف (Lifecycle) في جمعية مديم الرقمية والتي تشمل المراحل التالية:

- قبل التوظيف.
- خلال فترة العمل.
- عند انتهاء فترة العمل أو إنهائها.

4-1 يجب على العاملين في جمعية مديم الرقميةفهم أدوارهم الوظيفية، والشروط والمسؤوليات ذات العلاقة بالأمن السيبراني، والموافقة عليها.

5-1 يجب تضمين مسؤوليات الأمن السيبراني وبنود المحافظة على سرية المعلومات (Non-Disclosure Agreement) في عقود العاملين في جمعية مديم الرقمية (لتشمل خلال وبعد انتهاء/إنهاء العلاقة الوظيفية مع جمعية مديم الرقمية).

6-1 يجب إدراج المخالفات ذات العلاقة بالأمن السيبراني في لائحة مخالفات الموارد البشرية في جمعية مديم الرقمية.

7-1 يُمنع الاطلاع على المعلومات الخاصة بالموظفين دون تصريح مسبق.

8-1 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لمتطلبات الأمن السيبراني المتعلق بالموارد البشرية.

قبل التوظيف :

1-2 يجب على العاملين التعهد بالالتزام بسياسات الأمن السيبراني قبل منحهم صلاحية الوصول إلى أنظمة جمعية مديم الرقمية.

2-2 يجب تحديد أدوار الموظفين ومسؤولياتهم مع الأخذ في الحسبان تطبيق مبدأ عدم تعارض المصالح.

3-2 يجب تحديد أدوار الموظفين ومسؤولياتهم المتعلقة بالأمن السيبراني في الوصف الوظيفي.

4-2 يجب أن تشمل الأدوار والمسؤوليات المتعلقة بالأمن السيبراني مايلي:

- حماية جميع أصول جمعية مديم الرقمية من الوصول غير المصرح به، أو تخريب تلك الأصول.
- تنفيذ جميع الأنشطة المطلوبة المتعلقة بالأمن السيبراني.
- الالتزام بسياسات الأمن السيبراني ومعاييره الخاصة بـجمعية مديم الرقمية.
- الالتزام ببرنامج زيادة مستوى الوعي بالمخاطر السيبرانية.

5-2 يجب إجراء مسح أمني للعاملين في وظائف الأمن السيبراني، والوظائف التقنية ذات الصلاحيات الهامة والحساسة، والوظائف ذات العلاقة بالأنظمة الحساسة.

أثناء العمل :

1-3 يجب تقديم برنامج توعوي، يختص بزيادة مستوى الوعي بالأمن السيبراني؛ بما في ذلك سياسات الأمن السيبراني ومعاييره، بشكل دوري.

2-3 يجب على مسؤول الموارد البشرية إبلاغ الإدارات ذات العلاقة عن أي تغيير في أدوار العاملين أو مسؤولياتهم بهدف اتخاذ الإجراءات اللازمة المتعلقة بإلغاء صلاحيات الوصول أو تعديلها.

3-3 يجب التأكد من تطبيق متطلبات الأمن السيبراني الخاصة بالموارد البشرية.

4-3 يجب إدراج مدى الالتزام بالأمن السيبراني ضمن جوانب تقييم الموظفين.

5-3 يجب التأكد من تطبيق مبدأ الحاجة إلى المعرفة (Need-to-know) في تكليف المهمات.

انتهاء الخدمة أو إنهاؤها :

1-4 يجب تحديد إجراءات انتهاء الخدمة المهنية أو إنهائها بشكل يغطي متطلبات الأمن السيبراني.

2-4 يجب على مسؤول الموارد البشرية إبلاغ الوحدات ذات العلاقة في حال اقتراب موعد انتهاء العلاقة الوظيفية أو إنهائها لاتخاذ الإجراءات اللازمة.

3-4 يجب التأكد من إعادة جميع الأصول الخاصة بـجمعية مديم الرقمية وإلغاء صلاحيات الدخول للعاملين في آخر يوم عمل لهم وقبل حصولهم على المخالصات اللازمة.

4-4 يجب تحديد المسؤوليات والواجبات التي ستبقى سارية المفعول بعد انتهاء خدمة العاملين في جمعية مديم الرقمية، بما في ذلك اتفاقية المحافظة على سرية المعلومات، على أن يتم إدراج تلك المسؤوليات والواجبات في جميع عقود العاملين.

الأدوار والمسؤوليات :

1. راعي ومالك وثيقة السياسة: مسؤول تقنية المعلومات
2. مراجعة السياسة وتحديثها: مسؤول تقنية المعلومات
3. تنفيذ السياسة وتطبيقها: مسؤول الموارد البشرية

الالتزام بالسياسة :

1. يجب على مسؤول تقنية المعلومات ضمان التزام جمعية مديم الرقمية بهذه السياسة دورياً.
2. يجب على جميع العاملين في جمعية مديم الرقمية الالتزام بهذه السياسة.
3. قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة، إلى إجراء تأديبي؛ حسب الإجراءات المتبعة في جمعية مديم الرقمية .