

## ٦-سياسة النشر الإلكتروني (أمن البريد الإلكتروني)

المسؤول عنها	الاتصال المؤسسي
رمز السياسة	إعلام.س.٦
الحالة	معتمدة

### -الاعتماد

الحمد لله والصلاة والسلام على رسول الله وبعد:  
فقد اطلع أعضاء الجمعية العمومية بجمعية مكافحة السرطان الخيرية بالأحساء (تفاؤل)  
في اجتماعهم العادي يوم الإثنين الموافق ٢٠٢٢/٩/١٩م على **سياسة النشر الإلكتروني**  
وقرروا اعتمادها والعمل بموجبها ونشرها على الموقع الإلكتروني للجمعية وفق الصيغة  
المرفقة بالاعتماد.

رئيس مجلس الإدارة

محمد بن عبد العزيز العفالق

## أمن البريد الإلكتروني:

### الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية البريد الإلكتروني لجمعية مكافحة السرطان (تفاؤل) 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 (٢-٤-١) من الضوابط الأساسية للأمن السيبراني (١:١٨-٢-ECC) الصادرة من الهيئة الوطنية للأمن السيبراني.

### نطاق العمل وقابلية التطبيق:

تغطي هذه السياسة جميع أنظمة البريد الإلكتروني الخاصة بجمعية مكافحة السرطان (تفاؤل) وتنطبق على جميع العاملين في جمعية مكافحة السرطان (تفاؤل).

### بنود السياسة:

١. يجب توفير تقنيات حديثة لحماية البريد الإلكتروني وتحليل وتصفية ( Filtering رسائل البريد الإلكتروني وحظر الرسائل المشبوهة مثل: الرسائل الاقترامية ( Emails Spam) ورسائل التصيد الإلكتروني ( Emails Phishing).

٢. يجب أن تستخدم أنظمة البريد الإلكتروني أرقام تعريف المستخدم وكلمات المرور مرتبطة، لضمان عزل اتصالات المستخدمين المختلفين.

٣. يجب توفير التقنيات اللازمة لتشفير البريد الإلكتروني الذي يحتوي على معلومات مصنفة.

٤. يجب تطبيق خاصية التحقق من الهوية متعدد العناصر ( Authentication Multi Factor- للدخول عن بعد والدخول عن طريق صفحة موقع البريد الإلكتروني ( Webmail ) ).

٥. يجب أرشفة رسائل البريد الإلكتروني والقيام بالنسخ الاحتياطي دورياً.

٦. يجب تحديد مسؤولية البريد الإلكتروني للحسابات العامة والمشاركة ( Account Generic )

٧. 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.

٨. يجب توثيق مجال البريد الإلكتروني لجمعية مكافحة السرطان (تفاؤل) عن طريق استخدام الوسائل اللازمة؛ مثل طريقة إطار سياسة المرسل ( Sender Policy Framework ) لمنع تزوير البريد الإلكتروني ( Email Spoofin ) . كما يجب التأكد من موثوقية مجالات رسائل البريد الواردة ( DMARC Incoming message verification. ) .

٩. يجب أن يقتصر الوصول إلى رسائل البريد الإلكتروني على العاملين لدى جمعية مكافحة السرطان (تفاؤل).

١٠. يجب اتخاذ الإجراءات اللازمة؛ لمنع استخدام البريد الإلكتروني لجمعية مكافحة السرطان (تفاؤل) في غير أغراض العمل.

١١. يمنع وصول مسؤول النظام ( System Administrator ) إلى معلومات البريد الإلكتروني الخاصة بأي موظف دون الحصول على تصريح مسبق.

١٢. 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.

١٣.. يجب تذييل رسائل البريد الإلكتروني المرسلة إلى خارج جمعية مكافحة السرطان (تفاؤل) بإشعار إخلاء المسؤولية.

١٤.. يجب تطبيق التقنيات اللازمة؛ لحماية سرية رسائل البريد الإلكتروني وسالمتها، وتوافرها أثناء نقلها وحفظها؛ وتشمل هذه الإجراءات استخدام تقنيات التشفير وتقنيات منع تسريب البيانات.

١٥.. يجب استخدام مؤشر قياس الأداء ( KPI ) لضمان التطوير المستمر لنظام البريد الإلكتروني.

١٦.. يجب تعطيل خدمة تحويل البريد الإلكتروني من الخادم ( Op Mail Relay ).

### الأدوار والمسؤوليات:

١. راعي ومالك وثيقة السياسة: مسؤول تقنية المعلومات.
٢. مراجعة السياسة وتحديثها: مسؤول تقنية المعلومات.
٣. تنفيذ السياسة وتطبيقها: مسؤول تقنية المعلومات.

### الالتزام بالسياسة

١. يجب على مسؤول تقنية المعلومات ضمان التزام جمعية مكافحة السرطان (تفاؤل) بهذه السياسة بشكل دوري.
٢. يجب على جميع العاملين في جمعية مكافحة السرطان (تفاؤل) الالتزام بهذه السياسة.
٣. قد يُعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي؛ حسب الإجراءات المتبعة في جمعية مكافحة السرطان (تفاؤل).

