جمعية طهور بعنيزة
Tahoor Association in Onaizah
إدارة التطوير – مشروع التميز المؤسسي

سياسة إدارة التقنية وأمن المعلومات

اعتمدت هذه السياسة في اجتماع مجلس الإدارة (٢) لعام ٢٠٢٢م في ١٨/ ٠٨/ ١٤٤٣هـ الموافق ٢١/ ٠٣/ ٢٠٢٢م
وتم اعتماد هذه النسخة في الاجتماع (٣) لعام ٢٠٢٦ في ٢٢/ ٠٢/ ١٤٤٨هـ الموافق ٠٥/ ٠٨/ ٢٠٢٦م

النسخة الثانية

سياسة تميز:	14	**رقم الإصدار**	02	**عدد الصفحات**	7
تاريخ الإصدار	21/ 03/ 2022		**تاريخ التعديل**	05/ 08/ 2026	

جمعية طهور بعنيزة
وثيقة داخلية معتمدة
ترخيص رقم 618
Tahoor Association in Onaizah

سياسة إدارة التقنية وأمن المعلومات

أولا – المقدمة:

تشهد البيئة التقنية تطورًا متسارعًا في مختلف المجالات، الأمر الذي يجعل من إدارة التقنية وأمن المعلومات عنصرًا أساسيًا لضمان استقرار الأعمال ورفع كفاءة الأداء المؤسسي. وفي هذا السياق، تأتي هذه السياسة كإطار منظم يحكم الممارسات التقنية داخل جمعية طهور، ويحدد المبادئ العامة التي تُبنى عليها إدارة وتشغيل وتطوير البنية التحتية التقنية والأنظمة الرقمية.

وتسعى هذه السياسة إلى ترسيخ ممارسات حوكمة تقنية فعّالة، تضمن الاتساق بين الأنظمة، وحسن إدارة الموارد التقنية، وتعزيز موثوقية الخدمات الرقمية المقدمة داخل الجمعية. كما تؤكد على أهمية الالتزام بالضوابط والمعايير المعتمدة في مجال تقنية المعلومات وأمن المعلومات، بما يسهم في رفع مستوى الانضباط التشغيلي، ودعم استمرارية الأعمال، وتحقيق الاستخدام الأمثل للموارد التقنية..

ثانيا – الغرض من السياسة:

تهدف هذه السياسة إلى وضع إطار عام يحكم إدارة التقنية وأمن المعلومات في جمعية طهور، بما يضمن اختيار التقنيات المناسبة وتوظيفها بالشكل الأمثل لدعم استراتيجية الجمعية وتحقيق أهدافها. كما تسعى السياسة إلى تطوير البنية التحتية التقنية ومواكبة التحول الرقمي ومستجدات الثورة الصناعية الرابعة، بما يعزز جودة الخدمات المقدمة للمستفيدين والمعنيين، ويدعم جهود الإبداع والابتكار والتحسين المستمر.

وتؤكد السياسة على ضمان التكامل والتوافق بين الأنظمة التقنية، ومع الحرص على الاستخدام الأمثل للموارد المتاحة إلى جانب قياس مدى الاستفادة منها، كما أنها تؤكد على حماية أنظمة المعلومات والحفاظ على فعالية الضوابط الأمنية وتحسينها بشكل مستمر وفق المواصفات القياسية ذات العلاقة..

ثالثا – التعريفات:

١) التقنية (Technology): مجموعة الأنظمة والأدوات والحلول الرقمية والتطبيقات والبنية التحتية المستخدمة لدعم عمليات الجمعية وتحقيق أهدافها.

٢) تقنية المعلومات (IT): إدارة وتشغيل وتطوير الأنظمة الحاسوبية والشبكات وقواعد البيانات والبرمجيات والخدمات التقنية داخل الجمعية.

٣) أمن المعلومات (Information Security): مجموعة الإجراءات والضوابط التي تهدف إلى حماية البيانات والأنظمة التقنية من الوصول غير المصرح به أو الفقد أو التعديل أو الإتلاف.

٤) التحول الرقمي (Digital Transformation): عملية تحويل الخدمات والعمليات التقليدية إلى خدمات رقمية تعتمد على التقنيات الحديثة لرفع الكفاءة وتحسين تجربة المستفيد.

٥) البنية التحتية التقنية (IT Infrastructure): جميع المكونات التقنية المادية والبرمجية مثل الشبكات، الخوادم، الأجهزة، الأنظمة، المنصات، والموقع الإلكتروني.

٦) الأنظمة التقنية (Systems): البرمجيات والتطبيقات والمنصات الرقمية المستخدمة في تشغيل أعمال الجمعية (مثل نظام رافد والأنظمة الداخلية).

٧) الأصول التقنية (IT Assets): جميع الموارد التقنية المملوكة أو المُدارة من الجمعية وتشمل الأجهزة، البرمجيات، التراخيص، الشبكات، وقواعد البيانات.

٨) الحادث الأمني (Security Incident): أي حدث يؤدي أو قد يؤدي إلى اختراق أو تهديد أو تعطيل أو تسريب أو فقدان بيانات أو أنظمة الجمعية.

٩) استمرارية الأعمال (Business Continuity): القدرة على استمرار تقديم الخدمات الأساسية للجمعية أثناء وبعد حدوث أعطال أو كوارث تقنية أو أمنية.

١٠) التكامل التقني (Systems Integration): قدرة الأنظمة التقنية المختلفة على العمل معًا وتبادل البيانات بشكل متناسق وفعّال.

١١) الكفاءة التقنية (IT Efficiency): مدى الاستخدام الأمثل للموارد التقنية لتحقيق أعلى استفادة تشغيلية بأقل تكلفة وجهد ممكن.

١٢) إدارة الحوادث التقنية (Incident Management): الإجراءات المنظمة لاكتشاف الحوادث التقنية أو الأمنية وتسجيلها ومعالجتها وإغلاقها وفق أطر زمنية محددة..

رابعا – السياسات (الالتزامات)

٤-١: تلتزم الجمعية بتبني آلية واضحة لحسن اختيار التقنيات المناسبة والمطلوبة لمتطلبات المنظمة ومواكبة المتغيرات المتسارعة في التقنيات المختلفة.

٤-٢: الالتزام بإدارة وتشغيل التقنية لدعم تنفيذ استراتيجية الجمعية وتهيئة كافة الموارد التقنية والفنية لتقديم خدمات إلكترونية لكافة الوحدات الداخلية وكافة فئات المعنيين.

٤-٣: تلتزم جمعية طهور بتطوير البنية التحتية للتكنولوجيا وتشمل (المنصات الشبكة الداخلية والموقع الإلكتروني) لدعم أنشطة المنظمة وعملياتها الداخلية والخارجية

٤-٤: الالتزام بتبني مفهوم واستراتيجية التحول الرقمي والثورة الصناعية الرابعة ومكوناتها مثل (الحوسبة السحابية وإنترنت الأشياء والمستشعرات الذكية وتحليل البيانات الضخمة وغيرها) في تطوير وتحسين الخدمات المقدمة للمستفيدين.

٤-٥: تقوم الجمعية تيسير استخدام التقنية الحديثة وتقنية المعلومات لدعم جهود التطوير والتحسين المستمر لأدائها، ودعم جهود الإبداع والابتكار التي تقود عمليات التطوير والتحسين.

٤-٦: تلتزم الجمعية بإدارة أنظمتها التقنية وتشغيلها بما يضمن توافقها وتكاملها مع بعضها، مع الحرص على تحديث ما يتقادم منها.

٤-٧: تلتزم الجمعية باستخدام تقنياتها الحالية بأقصى كفاءة ممكنة، ومتابعة قياس مدى الاستفادة الفعلية منها بشكل دوري.

٤-٨: تلتزم الجمعية باستخدام تقنية المعلومات والاتصال لتحسين أدائها، والتأكد من الاستغلال الأمثل للموارد التقنية ومراجعة جدوى الاستثمار فيها.

٤-٩: تلتزم جمعية طهور بحماية أنظمة المعلومات لديها، والقيام بإجراء تحسين مستمر لها؛ للحفاظ على فعالية الضوابط الأمنية وتحسينها، وتبني المواصفات القياسية ذات العلاقة.

خامسا – الأدوار والمسؤوليات

١) مجلس الإدارة: اعتماد السياسة وتوفير الموارد اللازمة لتنفيذها، ومراجعة التقارير الدورية
٢) المدير التنفيذي: الإشراف على تنفيذ السياسة وتوافقها مع استراتيجية الجمعية، واعتماد المبادرات التقنية، ومتابعة الأداء.
٣) إدارة التطوير – تقنية المعلومات: اختيار الحلول التقنية المناسبة، وإدارة وتشغيل البنية التحتية التقنية، ومتابعة كفاءة استخدامها وتحديث ما يتقادم منها.
٤) مدراء الإدارات: تحديد الاحتياجات التقنية لوحداتهم، والتعاون مع إدارة التقنية لتفعيل الخدمات، والإبلاغ عن أي مشكلات تقنية.
٥) الموظفون: الاستخدام السليم للأنظمة والموارد التقنية، والالتزام بالضوابط الأمنية، والإبلاغ عن أي مخالفات أو أعطال.

سادسا – المستندات الواجب توافرها:

١) دليل أو إجراء إدارة وتشغيل الأنظمة التقنية
٢) سجل الأصول التقنية (حصر الأجهزة، الأنظمة، التراخيص، وحالتها التقنية والعمرية)
٣) خطة إدارة وتحديث المنظومة التقنية
٤) إجراءات وضوابط أمن المعلومات (سياسة كلمات المرور، الصلاحيات، النسخ الاحتياطي، إلخ)
٥) خطة الاستجابة للحوادث الأمنية
٦) خطة استمرارية الأعمال والتعافي من الكوارث
٧) نموذج/ سجل تقييم المخاطر التقنية
٨) مؤشرات قياس الأداء التقني لقياس مدى استغلال الأنظمة وكفاءتها.
٩) سجل حوادث ومخالفات أمن المعلومات

سابعا – النطاق (المستفيدون والمستهدفون من السياسة):

تسري هذه السياسة على جميع الإدارات والأقسام في جمعية طهور، وتشمل كافة الموظفين والمتعاقدين والمستفيدين من الخدمات التقنية، وتغطي جميع الأنظمة والبنية التحتية التقنية المملوكة أو المُدارة من قِبل الجمعية (بما في ذلك نظام رافد، المنصات الإلكترونية، الشبكة الداخلية، الموقع الإلكتروني، وقواعد البيانات)، كما تشمل جميع العمليات المرتبطة بإدارة التقنية وتشغيلها، من اختيار التقنيات وتطويرها، وحماية أنظمة المعلومات، وصولاً إلى تقديم الخدمات الإلكترونية لكافة الوحدات الداخلية والمستفيدين، وذلك في مقر الجمعية الرئيسي دون وجود فروع أخرى تابعة لها.

ثامنا – تطبيق السياسة:

يهدف هذا القسم إلى تحديد الآليات التنفيذية لتطبيق سياسة إدارة التقنية وأمن المعلومات داخل الجمعية، من خلال خطوات عملية واضحة تُترجم الالتزامات والسياسات إلى ممارسات تشغيلية، بما يضمن كفاءة التشغيل، واستمرارية الخدمات، ورفع مستوى الامتثال للضوابط المعتمدة.

م	الخطوات	المسؤولية	الزمن	قياس الفعالية
١	تحديد مواءمة التقنيات والحلول مع احتياجات الجمعية والاستراتيجية واعتمادها	إدارة تقنية المعلومات + المدير التنفيذي	عند كل مشروع / سنوي	نسبة مواءمة التقنيات مع الاحتياج والاستراتيجية

م	الخطوات	المسؤولية	الزمن	قياس الفعالية
٢	التخطيط واعتماد المشاريع التقنية بما يضمن دعم استراتيجية الجمعية	إدارة تقنية المعلومات + المدير التنفيذي	سنوي / عند التحديث	نسبة مواءمة المشاريع مع الاستراتيجية
٣	تشغيل وإدارة الأنظمة والخدمات التقنية وضمان استمرارية العمل	إدارة تقنية المعلومات	يومي / مستمر	نسبة توفر الأنظمة والخدمات (Uptime)
٤	تطوير وتحديث البنية التحتية التقنية (شبكات، منصات، موقع إلكتروني)	إدارة تقنية المعلومات	ربع سنوي	نسبة تحديث البنية التحتية التقنية
٥	تنفيذ مبادرات التحول الرقمي وتبني التقنيات الحديثة (سحابة، ذكاء اصطناعي، بيانات)	إدارة تقنية المعلومات	حسب المشاريع	نسبة تبني تقنيات التحول الرقمي
٦	تحسين كفاءة استخدام الأنظمة التقنية ورفع الاستفادة منها	إدارة تقنية المعلومات	نصف سنوي	نسبة كفاءة استخدام الأنظمة التقنية
٧	ضمان تكامل الأنظمة التقنية وتحديثها المستمر ومعالجة التقادم	إدارة تقنية المعلومات	ربع سنوي	نسبة تكامل وتحديث الأنظمة
٨	متابعة وتحليل الاستفادة الفعلية من التقنيات المستخدمة ورفع كفاءة الاستثمار	إدارة تقنية المعلومات	نصف سنوي	نسبة الاستفادة الفعلية من التقنية
٩	تطبيق ضوابط وسياسات أمن المعلومات (صلاحيات، كلمات مرور، نسخ احتياطي)	إدارة تقنية المعلومات	مستمر	نسبة الالتزام بسياسات أمن المعلومات
١٠	إدارة الحوادث الأمنية وتنفيذ اختبارات استمرارية الأعمال والتعافي	إدارة تقنية المعلومات	عند الحاجة + سنوي	عدد الحوادث المغلقة + نجاح اختبارات الاستمرارية

تاسعا – القياس:

يهدف هذا القسم إلى قياس مدى فاعلية تطبيق سياسة إدارة التقنية وأمن المعلومات من خلال مؤشرات أداء كمية ونوعية، تسهم في متابعة مستوى الالتزام، وتقييم كفاءة الأداء التقني، ودعم اتخاذ القرار والتحسين المستمر.

م	المؤشر	المستهدف	الاستفادة من القياس	كيفية القياس
١	نسبة مواءمة التقنيات والحلول المختارة مع احتياجات الجمعية	≥ 90%	ضمان اختيار تقنيات مناسبة تدعم احتياجات العمل (يرتبط بالبند ١)	مراجعة قرارات الاعتماد التقنية ومحاضر الاختيار
٢	نسبة مواءمة المشاريع التقنية مع استراتيجية الجمعية	≥ 90%	قياس دعم التقنية للاستراتيجية (يرتبط بالبند ٢)	مراجعة خطط المشاريع واعتمادها من الإدارة العليا
٣	نسبة توفر الخدمات والأنظمة التقنية (Uptime)	≥ 99%	ضمان استمرارية الخدمات الإلكترونية (يرتبط بالبند ٢ و٣)	أدوات مراقبة الأنظمة وتقارير التشغيل
٤	نسبة تحديث البنية التحتية التقنية (شبكات، منصات، موقع)	≥ 95%	قياس تطوير وتحديث البنية التحتية (يرتبط بالبند ٣)	تقارير التحديث والصيانة الدورية
٥	نسبة تبني تقنيات التحول الرقمي (سحابة، ذكاء اصطناعي، بيانات)	≥70% من المبادرات	قياس التحول الرقمي ومواكبة التقنية الحديثة (يرتبط بالبند ٤)	تقارير المشاريع التقنية ومؤشرات التحول الرقمي

م	المؤشر	المستهدف	الاستفادة من القياس	كيفية القياس
٦	نسبة كفاءة استخدام الأنظمة التقنية	≥ 80%	رفع كفاءة الاستثمار التقني (يرتبط بالبند ٥)	تحليلات الاستخدام وتقارير الأنظمة
٧	نسبة التزام الأنظمة بالتكامل والتحديث المستمر	≥ 90%	ضمان تكامل الأنظمة وعدم تقادمها (يرتبط بالبند ٦)	تقارير التكامل الفني وإدارة الأنظمة
٨	نسبة تحقيق الاستفادة الفعلية من التقنيات المستخدمة	≥ 80%	قياس العائد التشغيلي من التقنية (يرتبط بالبند ٧ و٨)	تقارير الاستخدام + دراسات العائد
٩	نسبة الالتزام بسياسات أمن المعلومات	≥ 95%	حماية البيانات والأنظمة (يرتبط بالبند ٩)	تقارير التدقيق الأمني وسجلات الامتثال
١٠	عدد الحوادث الأمنية المغلقة وفق الإجراءات النظامية	100%معالجة	تعزيز الحوكمة الأمنية وتقليل المخاطر (يرتبط بالبند ٩)	سجل الحوادث ونظام إدارة التذاكر الأمنية

عاشرا – المخرجات المتوقعة:

١) حوكمة تقنية واضحة: خطط ومشاريع تقنية معتمدة ومرتبطة باستراتيجية الجمعية.
٢) تشغيل مستقر: أنظمة وبنية تحتية تعمل بكفاءة مع استمرارية عالية للخدمات وتقليل الأعطال.
٣) أمن معلومات فعّال: تطبيق ضوابط الحماية، إدارة الحوادث، وتقليل المخاطر الأمنية.
٤) كفاءة واستثمار أفضل للتقنية: رفع استخدام الأنظمة وتحسين العائد وتقليل الهدر.
٥) تحسين مستمر قائم على القياس: تقارير ومؤشرات أداء دورية تدعم اتخاذ القرار والتطوير المستمر..

حادي عشر – التطوير:

تخضع هذه السياسة للمراجعة والتطوير بشكل دوري لضمان مواءمتها مع التطورات التقنية، واحتياجات الجمعية، وأفضل الممارسات في مجال تقنية المعلومات وأمن المعلومات. ويتم تحديثها في الحالات التالية:

١) عند حدوث تغييرات جوهرية في البنية التقنية أو الأنظمة المستخدمة .
٢) عند صدور أنظمة أو لوائح تنظيمية جديدة ذات علاقة .
٣) بناءً على نتائج القياس ومؤشرات الأداء أو تقارير التدقيق .
٤) عند ظهور مخاطر تقنية أو أمنية تتطلب تعديل الضوابط والسياسات .
٥) بشكل دوري لا يقل عن مرة كل (سنتين) كحد أقصى .

وتتم عملية التطوير بمشاركة إدارة تقنية المعلومات، وإدارة التطوير، واعتمادها من مجلس الإدارة.

ثاني عشر – المراجع:

١) اللائحة الأساسية للجمعية
٢) نظام حماية البيانات والأنظمة في المملكة العربية السعودية.
٣) ضوابط الأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني.
٤) معيار إدارة أمن المعلومات ISO/ IEC 27001.
٥) أفضل ممارسات إدارة خدمات تقنية المعلومات.
٦) اللوائح والسياسات الداخلية المعتمدة في جمعية طهور.

٧) دليل حوكمة وإدارة تقنية المعلومات في المنظمات غير الربحية
٨) سياسة خصوصية البيانات.

ثالث عشر – الاعتماد:

تم اعتماد هذه النسخة في اجتماع مجلس إدارة رقم (٣) لعام ٢٠٢٦م في ٢٢/ ٠٢/ ١٤٤٨هـ الموافق ٠٥/ ٠٨/ ٢٠٢٦م، ويسري العمل بها من تاريخ اعتمادها.

رئيس مجلس الإدارة

أنس بن محمد السليم