الهيئة العامة للعناية بشؤون المسجد الحرام والمسجد النبوي

سياسة الاستخدام المقبول

اسم المنظمة	الهيئة العامة للعناية بشؤون المسجد الحرام والمسجد النبوي
اسم الوثيقة	سياسة الاستخدام المقبول
تصنيف الوثيقة	مقيد
رقم آخر إصدار	٤,٠
نوع الوثيقة	إصدار
مالك الوثيقة	الإدارة العامة للأمن السيبراني

نسخة الوثيقة

النسخة	التاريخ	بواسطة	الدور	الإدارة
V1	١٤٤١/١/١هـ	تركي سعد الزهراني	سياسة جديدة	الحوكمة الرقمية
	١٤٤١/١/١هـ	م. رائد محمد المطرفي	مراجعة وتدقيق	الإدارة العامة للأمن السيبراني
V2	١٤٤٢/٤/٣٠هـ	م. عايض بن هندي هنيدي المجنوني	تحديث	الحوكمة الرقمية
	١٤٤٢/٥/١	مناع بن جمعان الغامدي	مراجعة وتدقيق	
V3	١٤٤٣/٨/٢٠هـ	مناع بن جمعان الغامدي	تحديث	الحوكمة الرقمية
	١٤٤٣/٨/٢٥هـ	سعد بن حسن الشمراني	مراجعة وتدقيق	الإدارة العامة للأمن السيبراني
	١٤٤٣/١١/١هـ	عبد الإله بن محمد الخزيم	مراجعة وتدقيق	إدارة الشؤون القانونية
V4	١٤٤٥/٦/٣٠هـ	سعد بن حسن الشمراني	تحديث	الحوكمة الرقمية
	١٤٤٥/٧/٤هـ	تركي بن سعد الزهراني	مراجعة وتدقيق	

المحتويات

١. المقدمة

تمثل هذه الوثيقة سياسة الاستخدام المقبول لدى الهيئة العامة للعناية بشؤون المسجد الحرام والمسجد النبوي والمُشار إليها داخل هذه الوثيقة.

تتكون هذه الوثيقة من تسعة أقسام رئيسية لتشمل هذه المقدمة يليها الغرض والنطاق، والأدوار والمسئوليات، والمصطلحات والتعريفات، وبنود السياسة والمرجعيات والالتزام وأخيراً معايير الاستثناءات.

على جميع المستخدمين القيام بالقراءة المتأنية والفهم الجيد والالتزام الكامل بسياسة الاستخدام المقبول، وفي حالة عدم الاستيعاب أو عدم الفهم الكامل من قِبَل المستخدم لهذه الوثيقة أو لأي جزء منها، فإنه يجب عليه التواصل مع الإدارة العامة للأمن السيبراني، وتعد الإدارة العامة للأمن السيبراني هي المالكة لهذه الوثيقة.

يجب على الإدارة العامة للأمن السيبراني مراجعة وتحديث هذه الوثيقة مرة واحدة على الأقل كل عام، أو يمكن أيضا تحديثها فور حدوث أي تعديلات تتعلق بالمتطلبات التشريعية والتنظيمية ذات العلاقة، ويتم تغيير رقم إصدار الوثيقة حال القيام بأي تعديل سواء كان طفيفاً أو كبيراً، ويجب اعتماد تلك التحديثات أو التعديلات من قبل اللجنة الإشرافية للأمن السيبراني بالهيئة العامة للعناية بشؤون المسجد الحرام والمسجد النبوي.

٢. الغرض

تهدف هذه السياسة إلى تحديد أدوار ومسؤوليات واضحة للمستخدمين لضمان الحماية والحفاظ على سرية وسلامة وتوافر الأصول المعلوماتية والتقنية للهيئة العامة للعناية بشؤون المسجد الحرام خلال عمليات الوصول والاستخدام.

٣. النطاق

تنطبق هذه السياسة على كافة مستخدمي الأصول المعلوماتية والتقنية كالموظفين، سواء كانوا يعملون بصفة دائمة، أو مؤقتة، أو متعاقدين، أو موردين، وموظفي المقاولين لدى الهيئة العامة للعناية بشؤون المسجد الحرام والمسجد النبوي.

٤. المصطلحات والتعريفات

- الأمن السيبراني: حسب ما نص عليه تنظيم الهيئة الوطنية للأمن السيبراني، الصادر بالأمر الملكي رقم (٦٨٠١) وتاريخ (١٤٣٩/٢/١١هـ) فإن الأمن السيبراني هو حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات من أي اختراق، أو تعطيل، أو تعديل، أو دخول، أو استخدام، أو استغلال غير مشروع، ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك.
- NCA: الهيئة الوطنية للأمن السيبراني.
- ISO: المنظمة الدولية للمعايير (منظمة الأيزو).
- نظام إدارة أمن المعلومات (ISMS): نظام تطبيق معيار الايزو ٢٧٠٠١.
- ECC: الضوابط الأساسية للأمن السيبراني.
- الأصل: أي شيء ملموس أو غير ملموس له قيمة بالنسبة للجهة، وهناك أنواع كثيرة من الأصول بعضها تتضمن أشياء واضحة مثل: الأشخاص، والآلات، والمرافق، وبراءات الاختراع، والبرمجيات، والخدمات، ويمكن أن يشمل المصطلح أيضاً أشياء أقل وضوحاً مثل: المعلومات والخصائص (مثل: سمعة الجهة وصورتها العامة، أو المهارة والمعرفة).
- السرية: الاحتفاظ بقيود مصرح بها على الوصول إلى المعلومات والإفصاح عنها بما في ذلك وسائل حماية معلومات الخصوصية والملكية الشخصية.

- سلامة المعلومات: الحماية ضد تعديل أو تخريب المعلومات بشكل غير مصرح به، وتتضمن ضمان عدم الإنكار للمعلومات والموثوقية.
- التوافُر: ضمان الوصول إلى المعلومات والبيانات والأنظمة والتطبيقات واستخدامها في الوقت المناسب.
- حادِثة: انتهاك أمني بمخالفة سياسات الأمن السيبراني، أو سياسات الاستخدام المقبول، أو ممارسات، أو ضوابط، أو متطلبات الأمن السيبراني.
- التَحَقُّق: التأكد من هوية المستخدم أو العملية أو الجهاز، وغالباً ما يكون هذا الأمر شرطاً أساسياً للسماح بالوصول إلى الموارد في النظام.
- صلاحية المستخدم: خاصية تحديد والتأكد من حقوق/تراخيص المستخدم للوصول إلى بعض الموارد وكذلك أمن الأصول المعلوماتية والتقنية للجهة بصفة عامة وضوابط الوصول بصفة خاصة.
- ضابط: مقياس لتقييد ومعالجة المخاطر.
- المخاطر: المخاطر التي تمس عمليات أعمال الجهة (بما في ذلك رؤية الجهة، أو رسالتها، أو إداراتها، أو صورتها، أو سمعتها، أو أصول الجهة) أو الأفراد أو الجهات الأخرى أو الدولة، بسبب إمكانية الوصول غير المصرح به أو الاستخدام، أو الإفصاح، أو التعطيل، أو التعديل، أو تدمير المعلومات، أو نُظم المعلومات.
- الفرص: أي فرصة إيجابية غير مؤكدة يمكن أن تؤثر بشكل إيجابي على أهداف الجهة في حالة حدوثها.
- الثغرة: أي نوع من نقاط الضعف في نظام الحاسب الآلي، أو برامجه أو تطبيقاته، أو في مجموعة من الإجراءات، أو في أي شيء يجعل الأمن السيبراني عرضة للتهديد.
- التهديد: أي ظرف أو حدث من المحتمل أن يؤثر سلباً على أعمال الجهة (بما في ذلك مهمتها، أو وظائفها، أو مصداقيتها، أو سمعتها، أو أصولها، أو منسوبيها) مستغلا أحد أنظمة المعلومات عن طريق الوصول غير المصرح به إلى المعلومات أو تدميرها أو كشفها أو تغييرها أو حجب الخدمة. وأيضاً قدرة مصدر التهديد على النجاح في استغلال أحد نقاط الضعف الخاصة بنظام معلومات معين. وهذا التعريف يشمل التهديدات السيبرانية.
- الاحتمالية: احتمالية حدوث مخاطر أمن سيبراني.
- التأثير: مدى الخسارة الناجمة عن استغلال تهديد لثغرة أمنية.
- اختبارات الاختراق: ممارسة اختبار على نظام حاسب آلي، أو شبكة، أو تطبيق موقع إلكتروني، أو تطبيق.
- هجوم: أي نوع من الأنشطة الخبيثة التي تحاول الوصول بشكل غير مشروع أو جمع موارد النظم المعلوماتية، أو المعلومات نفسها، أو تعطيلها، أو منعها، أو تحطيمها، أو تدميرها.
- انتهاك أمني: الإفصاح عن أو الحصول على معلومات لأشخاص غير مصرح تسريبها أو الحصول عليها، أو انتهاك السياسة الأمنية السيبرانية للجهة بالإفصاح عن أو تغيير أو تخريب أو فقد شيء سواء بقصد أو بغير بقصد، ويقصد بالانتهاك الأمني الإفصاح عن أو الحصول على بيانات حساسة، أو تسريبها، أو تغييرها، أو تبديلها، أو استخدامها بدون تصريح (بما في ذلك مفاتيح التشفير وغيرها من المعايير الأمنية السيبرانية الحرجة.
- مسؤول الخطر (Risk Owner): الشخص أو الإدارة المسؤولة عن الخطر وكيفية التعامل معه وتحديد واختيار الضوابط اللازمة لمعالجة الخطر وتقليله إلى مستوى المخاطر المقبول ومتابعة معالجة الخطر مع جميع الأطراف المعنية.

- مستوى المخاطر المقبول (Risk Acceptance Level): هو مستوى المخاطر الذي يمكن للهيئة أن تتحمل حدوثه ويمكن قبوله والتعامل معه.
- نسبة المخاطر المتبقية (Residual risks): هي النسبة المتبقية من الخطر في حالة التعامل معه وتطبيق الضوابط اللازمة لمعالجته وتقليله والتي قد تنتج من عدم تطبيق الضوابط الكافية لمعالجة الخطر مما قد يؤدي إلى وجود نسبة متبقية من الخطر قد تحتاج إلى تطبيق وتنفيذ ضوابط أخرى لتقليل نسبة الخطر المتبقي إلى مستوى المخاطر المقبول.
- سجل المخاطر (Risk Register): هو سجل يحتوي على البيانات الهامة الخاصة بإدارة المخاطر مثل رقم أو كود الخطر وتصنيف الخطر قبل وبعد المعالجة ونسبة الخطر المتبقية ومسؤول الخطر وحالة الخطر.

٥. الأدوار والمسؤوليات

- الإدارة العامة للأمن السيبراني
  - إعداد ومراجعة سياسة الاستخدام المقبول.
  - مراجعة التطبيق والتنفيذ لسياسة الاستخدام المقبول.
  - التحقق من أي مخالفات تتعلق بالأمن السيبراني تم الإبلاغ عنها أو اكتشافها.
- الموظفين
  - الالتزام بتطبيق سياسة الاستخدام المقبول.
  - إبلاغ الإدارة العامة للأمن السيبراني عن أي أحداث أو نقاط ضعف أو حوادث.
- الإدارة العامة للموارد البشرية
  - مسؤولة التنسيق مع جميع الموظفين للتوقيع على السياسة.

٦. بنود السياسة

٦,١. الاستخدام المقبول للأصول التقنية

- يجب استخدام جميع الأصول المعلوماتية والتقنية لأغراض العمل فقط لإتمام المهام الخاصة بالعمل.

٦,٢. المسئولية عن الأصول المعلوماتية والتقنية

- يجب تحديد مالك جميع الأصول المعلوماتية والتقنية في قائمة سجل الأصول.
- يكون مالك الأصل مسؤولاً عن إدارة الأصول المعلوماتية والتقنية المملوكة له ويجب عليه ضمان حماية سريتها وسلامتها وتوافرها.
- سيصبح مالك الأصل مسؤولاً عن تفويض من يلزم لتشغيل الأصول المعلوماتية والتقنية، ويجب عليه أن يعتمد ويعطي الصلاحيات لكل المستخدمين والموظفين الذين يتوجب عليهم الوصول او استخدام أصوله التقنية والمعلوماتية لأغراض العمل.

٦,٣. إعادة الأصول المعلوماتية والتقنية عند الاستقالة أو إنهاء الخدمة

- يجب على الموظف حال إنهاء خدمته أو تقدمه بالاستقالة أن يعيد جميع الأصول المعلوماتية والتقنية إلى الهيئة العامة للعناية بشؤون المسجد الحرام والمسجد النبوي.
- يجب على الإدارة العامة لتقنية المعلومات أن تقوم بتهيئة (format) أي قرص صلب خاص بالحاسب الشخصي الخاص بالموظف قبل تسليمه لأي موظف آخر أو قبل حفظه للاستعمال لاحقاً.

- ستقوم الإدارة العامة لتقنية المعلومات بحذف جميع صلاحيات الوصول الخاصة بأي موظف تم إنهاء خدمته أو تقدم باستقالته وأي موظف ينتقل من إدارة إلى إدارة أخرى.

٦,٤. سياسة المكتب النظيف والشاشة الخالية

- يجب في حالة عدم تواجد الموظف المصرح له في مكتبه أو مكان عمله إزالة جميع الوثائق الورقية ووسائط تخزين البيانات، خاصة المعلومات والبيانات السرية من المكتب أو أي أماكن أخرى مثل الطابعات وأجهزة الفاكس وآلات التصوير وما إلى ذلك لضمان منع أي وصول غير مصرح به.
- يجب حفظ تلك المستندات والوسائط في أماكن آمنة مثل الخزائن المقفلة إذا اقتضت الحاجة.
- يجب حفظ أي وثائق سرية بعيدًا عند عدم الحاجة إليها خاصةً عندما يكون المكتب فارغًا (يفضل حفظها داخل خزانة أو خزانة مقاومة للحريق كخيار مثالي).
- يجب تطبيق سياسة المكتب النظيف والشاشة الخالية وذلك عند ترك أي موظف حاسبه الشخصي أو جهاز العمل في وضع تسجيل الدخول دون استخدام الجهاز لبعض الوقت.

٦,٥. مسؤولية المستخدم عن بيانات الهوية

- يمنع بشكل مباشر أو غير مباشر لأي مستخدم أو موظف السماح باستخدام بياناته مثل اسم المستخدم وبطاقة الدخول وحقوق الوصول والصلاحيات وكلمة المرور الخاصة به مع مستخدمين آخرين.
- يعتبر الموظف هو مالك حساب المستخدم الخاص به ويكون مسؤول عن استخدامه وعن أي معاملات أو أنشطة يتم القيام بها بواسطة هذا الحساب.
- يجب على جميع المستخدمين اختيار كلمة مرور معقدة للتأكد من أن كلمات المرور الخاصة بهم لن يتم توقعها أو اختراقها بسهولة.
- يجب تغيير كلمة المرور من قبل جميع الموظفين بعد تسجيل الدخول لأول مرة.
- يجب على المستخدمين استخدام حساباتهم فقط لأغراض العمل الخاصة بالهيئة العامة للعناية بشؤون المسجد الحرام والمسجد النبوي فقط، ويمنع استعمالها استعمال شخصي.

٦,٦. سياسة استخدام الإنترنت

- يجب الوصول إلى خدمات الإنترنت الخاصة بالهيئة العامة للعناية بشؤون المسجد الحرام والمسجد النبوي باستخدام الاعدادات والتطبيقات المثبتة والتأكد من إجراء آخر تحديث لها.
- يجب على الهيئة العامة للعناية بشؤون المسجد الحرام والمسجد النبوي أن تثبت خدمة وكيل الويب web proxy لتنقية جميع طلبات المستخدمين للوصول إلى الإنترنت والسماح فقط للطلبات ذات الصلة بأغراض العمل.
- يجب أن تكون الضوابط التالية قيد التطبيق فيما يخص خدمة الوصول إلى الإنترنت داخل الهيئة العامة للعناية بشؤون المسجد الحرام والمسجد النبوي:
  - يجب أن يَمنع الوصول المفلتر إلى الإنترنت المستخدمين من الوصول إلى أي مواقع إلكترونية أو أي عناوين URL ليس لها علاقة بالعمل في الهيئة، على سبيل المثال لا الحصر، المواد الإباحية، والسياسة، والكراهية، والتمييز، والعنف، والمحتوى الآخر المصنف بشكل مشابه.

- يجب أن يَمنع الوصول المفلتر أي مستخدمين من الوصول إلى أي مواقع ويب ضارة أو مشبوهة مبلغ عنها.
- يلزم التحكم في قدرة وصول المستخدمين إلى الخدمة ولابد أيضا من تسجيل الأنشطة (سواء تم الوصول إليها أو تم حظرها).

- يسمح بالوصول إلى شبكة الإنترنت فقط عبر شبكة الهيئة العامة للعناية بشؤون المسجد الحرام والمسجد النبوي وباستخدام البنية التحتية وجدار الحماية المناسبين.
- يمنع الوصول إلى الإنترنت بواسطة أجهزة المودم أو الإنترنت عبر الهاتف المحمول أو أي أجهزة أخرى بهدف الاتصال المباشر بالإنترنت.
- يحظر الوصول المجهول إلى أي مواقع ويب محظورة باستخدام بروكسيات الويب المثبتة بشكل شخصي أو برامج VPN وإذا تم اكتشاف ذلك يتم إبلاغ الإدارة العامة للأمن السيبراني للتحقق حول هذا الانتهاك بحق سياسات الأمن السيبراني داخل الهيئة العامة للعناية بشؤون المسجد الحرام والمسجد النبوي.
- لا يمكن للمستخدم أن يقوم بتنزيل أي برنامج على شبكة الإنترنت قبل الحصول على إذن مسبق من الإدارة العامة لتقنية المعلومات، ويمكن للإدارة العامة لتقنية المعلومات أن تقوم بتنزيل البرنامج وتثبيته وهذا في حالة اتضاح أن هذا البرنامج سيستخدم في أغراض العمل داخل الهيئة العامة للعناية بشؤون المسجد الحرام والمسجد النبوي.
- يجب أن ينظر المستخدم إلى أي معلومات واردة من مواقع لم يتم التحقق منها على أنها غير موثوقة.
- يكون المستخدم مسؤولا عن جميع الآثار المحتملة الناتجة عن أي دخول غير مصرح به أو استخدام لخدمات الإنترنت.
- يجب حظر المواقع الإلكترونية المرتبطة بالتصنيفات التالية: الروبوتاتbotnets، ومسجلي المفاتيح، والمواقع الإلكترونية الخبيثة، ومواقع التصيد الاحتيالي، وغيرها، لأنها من مصادر تهديدات الأمن السيبراني، وقد تؤدي إلى المساس بسرية وسلامة وتوافر الأصول المعلوماتية والتقنية بالهيئة العامة للعناية بشؤون المسجد الحرام والمسجد النبوي.

٦,٧. سياسة استعمال البريد الإلكتروني

- يجب استخدام حسابات وخدمات البريد الإلكتروني للهيئة العامة للعناية بشؤون المسجد الحرام لأعمال الهيئة فقط وليس للاستعمال الشخصي مثل:
  - عمليات الشراء غير المصرح بها.
  - نشر الآراء الشخصية ووجهات النظر حول الموظفين، أو الموردين، أو الشركاء، أو العملاء.
  - التسجيل في برامج التواصل الاجتماعي أو مجموعات المناقشة وغرف الدردشة على الإنترنت أو أي منتديات إلكترونية عامة إلا بعد الحصول على إذن من قبل الهيئة العامة للعناية بشؤون المسجد الحرام والمسجد النبوي.
- تحتفظ الهيئة العامة للعناية بشؤون المسجد الحرام والمسجد النبوي بحق الوصول والكشف عن جميع الرسائل لأي غرض بدون إشعار مسبق لأي موظف، وقد يقوم المشرفين بمراجعة مراسلات البريد الإلكتروني للهيئة العامة للعناية بشؤون المسجد الحرام بهدف التأكد من عدم وجود اختراقات أو مخالفات لسياسة الهيئة العامة للعناية بشؤون المسجد الحرام والمسجد النبوي للأمن السيبراني.
- يجب تدقيق جميع رسائل البريد الإلكتروني الواردة والصادرة سواء داخليًا أو خارجيًا.
- يحظر على جميع الموظفين استخدام أي عناوين بريد إلكتروني غير عناوين الهيئة العامة للعناية بشؤون المسجد الحرام والمسجد النبوي للبريد الإلكتروني في جميع أغراض العمل.

- يجب توقيع موظف الهيئة العامة للعناية بشؤون المسجد الحرام والمسجد النبوي على جميع رسائله الإلكترونية المرسلة من خدمات البريد الإلكتروني على أن تشمل الاسم الأول والأخير والمسمى الوظيفي والإدارة التابع لها.
- يمنع إرسال رسائل عبر حساب البريد الإلكتروني الخاص بأي مستخدم آخر.
- ينصح ألا يقوم الموظف بالنقر على أي روابط أو أن يفتح أي مرفقات لأي رسائل بريد إلكتروني تبدو مشبوهة أو غير مرغوب فيها.
- لا تقوم بالنقر على أي رابط داخل رسالة بريد إلكتروني تابعة لبنك ما أو شركة رغبةً منهم في تحديث بياناتك الشخصية، ولا تترك نفسك عرضة للخداع من قبل أي مرسل لمجرد امتلاكه بعض التفاصيل الخاصة بك فمن اليسير أن يتم جمع معلومات عنك من خلال صفحة الفيسبوك أو Linked-In أو أي مواقع تواصل اجتماعي أخرى، ادخل بدلا من ذلك على الموقع الرسمي للبنك أو للمؤسسة عن طريق كتابة عنوانهم الخاص بهم على متصفح الويب أو اتصل بالبنك عبر الهاتف.
- يجب على موظفي الهيئة العامة للعناية بشؤون المسجد الحرام والمسجد النبوي عدم إعادة إرسال رسالة بريد إلكتروني لأي عنوان خارجي إلا بعد الموافقة المسبقة لمالك المعلومة أو من أنشأها أو إذا كانت المعلومة عامة بطبيعتها وبشكل واضح.
- يجب على موظفي الهيئة العامة للعناية بشؤون المسجد الحرام والمسجد النبوي عدم فتح المرفقات بالبريد الإلكتروني إذا لم يتم فحصها بواسطة حلول أمن البريد إلا إذا كانت من مرسلين موثوق بهم.

٦,٨. مسؤولية النسخ الاحتياطي للبيانات والمعلومات

- يقع على عاتق جميع موظفي الهيئة العامة للعناية بشؤون المسجد الحرام والمسجد النبوي مسئولية أخذ نسخ احتياطية لبيانات ومعلومات عملهم.
- يستطيع جميع موظفي الهيئة العامة للعناية بشؤون المسجد الحرام والمسجد النبوي التابعين لكل إدارة الوصول إلى الملفات المشتركة الخاصة بهم.

٦,٩. الإبلاغ عن حوادث الأمن السيبراني

- يجب على جميع موظفي ومتعاقدي وموردي الهيئة العامة للعناية بشؤون المسجد الحرام والمسجد النبوي أن يقوموا بإبلاغ الإدارة العامة للأمن السيبراني حال حدوث، أو اكتشاف حوادث، أو نقاط ضعف، أو أحداث تخص الأمن السيبراني وذلك بهدف تنشيط إجراءات إدارة الحوادث والعمل على حلها في أقرب وقت ممكن حتى يتم تفادى تأثيراتها على بيئة العمل.
- يجب على أي مُبلّغ عن حوادث الأمن السيبراني أن يدلي بأي أحداث تخصها ونقاط الضعف وجميع التفاصيل المتوفرة لديه من أجل تسهيل عملية التحقيق الرقمي.
- يجب على جميع موظفي الهيئة العامة للعناية بشؤون المسجد الحرام والمسجد النبوي الإبلاغ عن أي حوادث أو معلومات تتعلق بهم من خلال القنوات التالية:
- عنوان البريد الإلكتروني للإدارة العامة للأمن السيبراني (security@gph.gov.sa / إدارة عمليات الأمن السيبراني).
- رقم الهاتف الخاص بالإدارة العامة للأمن السيبراني (٥٧٣٣٧٧٧/ تحويلة:٦٦٣١/ إدارة عمليات الأمن السيبراني).

٧. المرجعيات

- ضوابط الأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني
- ISO27001

٨. الالتزام

- يجب أن تتوافق جميع سياسات الأمن السيبراني مع الضوابط الأساسية للأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني (ECC-1:2018).
- يجب الالتزام بسياسات الأمن السيبراني من قبل جميع المستخدمين داخل الهيئة العامة للعناية بشؤون المسجد الحرام والمسجد النبوي، ويجب على جميع مدراء الإدارات والأقسام التأكد من الالتزام المستمر بتطبيق هذه السياسات والتوافق معها، وذلك عن طريق مراقبة ومتابعة تطبيقها داخل إداراتهم وأقسامهم.
- يجب مراجعة الالتزام بتطبيق هذه السياسات دورياً بواسطة الإدارة العامة للأمن السيبراني، كما يجب على الإدارة العليا اتخاذ كافة الإجراءات التصحيحية اللازمة حال حدوث أي انتهاك لهذه السياسات حسب النظام.

٩. معايير الاستثناءات

- تهدف هذه الوثيقة إلى تلبية جميع متطلبات حماية الأمن السيبراني، وبناءً عليه يجب تقديم طلب رسمي عند الحاجة إلى الحصول على استثناء، ويقدم الطلب للإدارة العامة للأمن السيبراني مع ذكر الحيثيات بوضوح، وعرض الفوائد المرجوة من هذا الاستثناء ليتم البت فيه ومنح الموافقة النهائية من قبل اللجنة الإشرافية للأمن السيبراني.
- تصل فترة الاستثناء لمدة عام واحد كحد أقصى، إلا أنه يمكن إعادة تقييم طلب الاستثناء وتجديد الموافقة عليه بحد أقصى ثلاث أعوام متتالية إذا اقتضى الأمر ولا يمكن تمديد العمل بالاستثناء لفترات أخرى بعد انتهاء الثلاثة أعوام.