سياسات أمن المعلومات	تاريخ بدء العمل بالسياسة	٢١ / ٧ / ١٤٤١هـ
	تاريخ آخر مراجعة	٢١ / ٧ / ١٤٤١هـ
اسم السياسة: سياسة العمل عن بعد	تاريخ المراجعة القادمة	١ / ١ / ١٤٤٢هـ
	عدد صفحات هذه السياسة	١ من ٢

- **الهدف:**

الغرض من هذه السياسة هو تحديد قواعد ومتطلبات الاتصال عن بعد بشبكة الرئاسة العامة لشؤون المسجد الحرام من أي مضيف (Host)، والتي تحد من التعرض المحتمل للأضرار التي قد تنجم عن الاستخدام غير المصرح به لموارد الرئاسة. الأضرار تشمل فقدان بيانات حساسة أو سرية، والملكية الفكرية، والأضرار التي قد تؤثر على السمعة والصورة العامة، والأضرار التي تؤثر على الأنظمة الداخلية.

- **مجال التطبيق:**

تنطبق هذه السياسة على جميع المستخدمين في الرئاسة العامة بما في ذلك على سبيل المثال لا الحصر، الموظفين والمتعاقدين والاستشاريين اللذين يستخدمون أجهزة حاسب آلي -شخصية أو مملوكة للرئاسة العامة - للاتصال بشبكة عن بعد.

- **أي ممارسة خارج هذه السياسة يرجى مراجعة الإدارة العامة لأمن المعلومات ومكافحة الجرائم المعلوماتية.**

تفاصيل السياسة:

١-سياسة الاتصال عن بعد (VPN)

١-١ الممارسات المقبولة

- للحصول على صلاحية الاتصال عن بعد يقوم الموظف بالتوقيع على نموذج طلب خاص بذلك والتعهد بعدم استخدام الاتصال إلا في حاجة العمل.
- أخذ موافقة إدارة أمن المعلومات في حال الحاجة لاستخدام أي موارد خارجية لأغراض العمل.
- تحديد الغرض من الاتصال عن بعد او الوصول الى الخوادم.
- ضمان الوصول الأمن للشبكة عن بعد من خلال التشفير وكلمات مرور قوية.
- يشترط أن يكون جهاز الموظف الراغب في الاتصال عن بعد يحتوي على برنامج للحماية من الفيروسات.
- في حال تم الاتصال بشبكة الرئاسة عن طريق جهاز حاسب آلي شخصي، فإنه من مسئولية المستخدم منع الوصول لبيانات وموارد الرئاسة من أي مستخدمين غير مصرح لهم.
- في حال عدم استخدام الاتصال فإنه سيتم قطع الاتصال بعد ٥ دقايق من الاتصال الغير نشط.
- جميع الاتصالات عن بعد بتقنية إل (VPN) يتم تشفيرها وحمايتها لضمان عدم اطلاع أشخاص غير مصرح لهم على بيانات الرئاسة.
- عند السماح للمقاول والجهات الخارجية بالدخول عن بعد إلى شبكة الرئاسة لإنهاء بعض الأعمال المناطة بهم لا بد من تحديد فترة زمنية يتم بعدها إنهاء صلاحية الدخول.
- الاتصال عن بعد عبر جهاز شخصي فإنه ينبغي تطبيق جميع سياسات الأمان أثناء الاتصال.
- الاحتفاظ بكافة عناوين الأجهزة (MAC) وتسجيلها ومتابعتها إذا لزم الأمر.

١-٢ الممارسات الممنوعة

- إفشاء معلومات الاتصال عن بعد الخاصة (اسم المستخدم، كلمة المرور، بيانات الاتصال) لأي شخص.
- عند اتصال جهاز بشبكة الرئاسة عن بعد فإنه يمنع اتصاله بأي شبكة أخرى إلى حين إنهاء الاتصال.
- القيام بأي نشاط أو عمل غير قانوني من خلال شبكة الرئاسة بواسطة مستخدم مصرح له أو غير ذلك.
- استخدام شبكات الرئاسة لغير أغراض العمل الرئيسية.
- استخدام الاتصال عن بعد في غير مهام العمل او خارج وقت الدوام الصباحي.
- إعطاء صلاحيات من غير الرجوع الى إدارة أمن المعلومات.

٢- سياسة الدخول من الأجهزة الشخصية

٢-١ الممارسات المقبولة

- استخدام قنوات تشفير الاتصال مثل "الشبكة الافتراضية الخاصة (VPN)" أو "بروتوكول طبقة المقابس الآمنة (SSL) " أو "حزمة بروتوكول الإنترنت الأمنية (IPsec)" عند الدخول إلى أنظمة الجهة من خلال أجهزة المستخدمين
- تقع على عاتقك المسؤولية عن الاستخدام الملائم لجميع الموارد المخصصة لك.
- التأكد من وضع الجهاز المحمول دائما في أماكن آمنه وعدم تركه الا بعد وضعه على الوضع الامن.
- في حال الانتهاء من العمل بالجهاز الشخصي يجب انهاء اتصال VPN.
- يجب أن تكون الأجهزة المحمولة محمية حماية كاملة وذلك بتوفير الحد الأدنى من شروط حماية المعلومات مثل برنامج الحماية من الفيروسات المحدث، جدار ناري مفعل خاص بالجهاز، وجود خاصية تشفير البيانات، التحديث الدائم لنظام التشغيل والبرامج الموجودة على الجهاز، عدم تحميل البرامج الغير أصلية على الجهاز لأنها قد تحتوي على برامج للتجسس أو برامج خبيثة.
- تحديد الموارد المسموح بالوصول لها (صلاحية الدخول المحدود).
- تطبيق سياسات كلمات المرور المركبة على الأجهزة الشخصية.
- مراقبة التحديثات الأمنية على الاجهزة الشخصية، بحيث يتم خلالها إرسال تنبيهات للمستخدمين لتثبيت التحديثات الأمنية خلال فترة زمنية محددة. يجب أيضا، على الإدارات المعنية فصل أي جهاز غير محدث.

٢-٢ الممارسات الممنوعة

- تفعيل خاصية مشاركة الملفات بين الأجهزة دون اذن مسبق.
- تخزين ملفات خاصة بالرئاسة على الأجهزة الشخصية.
- إعطاء أي صلاحية من غير اذن مسبق من إدارة أمن المعلومات.
- محاولة الوصول الى أجزاء ممنوع الوصول لها بالشبكة
- تنزيل أو استخدام الأدوات التي تستخدم عادة لمهاجمة أنظمة الأمن أو اختراق أنظمة الكمبيوتر.

إعداد	مراجعة		اعتماد
مدير إدارة أمن المعلومات	مدير عام الإدارة العامة لأمن المعلومات ومكافحة الجرائم المعلوماتية	وكيل الرئيس العام للترجمة والشؤون التقنية	الرئيس العام لشؤون المسجد الحرام والمسجد النبوي
تركي بن سعد الزهراني	م. راند بن محمد المطرقي	أحمد بن عبد العزيز الحميدي	د. عبد الرحمن بن عبد العزيز السديس