دليل إرشادات الوصول عن بعد للموارد التقنية

الإصدار	التاريخ	الإعداد	مستوى الخصوصية	الإعتماد
1.0	أغسطس 2024	دائرة تقنية المعلومات	عام	محافظ مسندم

قائمة المحتويات:

تعريفات

المحافظة: محافظة مسندم

الوصول عن بعد:(Remote Access) عملية الاتصال بالموارد التقنية والأنظمة الداخلية للمؤسسة من خارج شبكة العمل باستخدام الإنترنت أو تقنيات الاتصال الآمنة مثل الشبكات الافتراضية الخاصة.(VPN)

الموارد التقنية:(Technical Resources) تشمل الأنظمة، التطبيقات، قواعد البيانات، الخوادم، والمخازن السحابية الخاصة بالمؤسسة التي يتم استخدامها لإنجاز المهام الوظيفية أو تخزين البيانات.

الشبكات الافتراضية الخاصة:(VPN - Virtual Private Network) تقنية تتيح إنشاء اتصال آمن عبر الإنترنت من جهاز المستخدم إلى شبكة المؤسسة، مما يسمح بنقل البيانات بطريقة مشفرة ومحمية.

التحقق الثنائي:(2FA - Two-Factor Authentication) عملية أمان تستخدم للتحقق من هوية المستخدمين عبر تطبيق خطوة إضافية (مثل رمز يُرسل إلى الهاتف المحمول) بجانب إدخال اسم المستخدم وكلمة المرور.

الجهاز الشخصي:(Personal Device) أي جهاز إلكتروني (كمبيوتر محمول، هاتف ذكي، جهاز لوحي، إلخ) يمتلكه المستخدم ويستخدمه للوصول إلى موارد المؤسسة التقنية عن بعد.

الأمن السيبراني:(Cybersecurity) مجموعة من الممارسات والتقنيات المصممة لحماية الأنظمة والشبكات والبيانات من الهجمات الإلكترونية أو الاختراقات.

النظام الداخلي:(Internal System) أي نظام أو تطبيق موجود ضمن بيئة العمل المغلقة للشركة، ولا يمكن الوصول إليه إلا عبر قنوات اتصال آمنة مثل VPN أو طرق أخرى محمية.

السياسة الأمنية:(Security Policy) مجموعة من القواعد والإرشادات التي تضعها المؤسسة لضمان حماية بياناتها وأنظمتها عند الوصول إليها عن بعد.

مراقبة النشاط:(Activity Monitoring) عملية مراقبة وتتبع الأنشطة التي يقوم بها المستخدم عند الوصول إلى موارد المؤسسة التقنية لضمان الامتثال والحد من التهديدات الأمنية.

التحكم عن بعد:(Remote Control) استخدام برامج تتيح لمسؤولي تقنية المعلومات الوصول إلى جهاز المستخدم وإدارته عن بُعد لتقديم الدعم الفني أو حل المشكلات التقنية.

الدعم الفني:(Technical Support) الخدمات التي تقدمها فرق تقنية المعلومات للمستخدمين للمساعدة في حل المشكلات التقنية أو تقديم إرشادات حول استخدام الأنظمة والبرامج.

البيانات المشفرة:(Encrypted Data) البيانات التي تم تحويلها إلى صيغة غير مقروءة باستخدام تقنيات التشفير لضمان عدم الوصول إليها من قبل أطراف غير مصرح لها.

الخرق الأمني:(Security Breach) حادثة يتم فيها الوصول إلى الأنظمة أو البيانات الحساسة للمؤسسة من قبل جهة غير مصرح لها، مما قد يؤدي إلى تسريب أو سرقة المعلومات.

الأجهزة المعتمدة:(Approved Devices) الأجهزة التي توافق عليها المؤسسة للاستخدام عند الوصول عن بعد، وتكون مجهزة بالبرامج والتحديثات الأمنية المطلوبة لضمان الأمان.

نظام التذاكر:(Ticketing System) نظام إدارة طلبات الدعم الفني حيث يسجل المستخدمون المشاكل التي يواجهونها ويتلقون متابعة من قبل فريق الدعم حتى يتم حلها.

مقدمة

في ظل التحول الرقمي المتسارع وزيادة الاعتماد على التكنولوجيا الحديثة، أصبح الوصول عن بعد للموارد التقنية أحد الركائز الأساسية لضمان استمرارية الأعمال والمرونة في التعامل مع المهام اليومية. يوفر هذا

الدليل إرشادات شاملة لضمان الوصول الآمن والفعال للموارد التقنية من خارج بيئة العمل التقليدية، مع التركيز على حماية البيانات، وضمان سرية المعلومات، والحفاظ على سلامة الأنظمة.
يهدف هذا الدليل إلى توجيه الموظفين في كيفية الوصول إلى الموارد التقنية بطريقة آمنة، مع الالتزام بالسياسات والمعايير المعتمدة من قبل المحافظة. من خلال اتباع الإرشادات المذكورة، يمكن للمستخدمين تحقيق أقصى استفادة من التقنيات المتاحة مع تقليل المخاطر الأمنية المحتملة.

النطاق

يغطي هذا الدليل جميع الإجراءات والتوجيهات المتعلقة بالوصول عن بعد إلى الموارد التقنية للمحافظة. ويشمل نطاق الدليل الفئات التالية:

1. **المستخدمون المستهدفون:**
   - **الموظفون الدائمون :**العاملون في المحافظة الذين يحتاجون إلى الوصول إلى الأنظمة والبيانات من خارج بيئة العمل التقليدية.
   - **المتعاقدون والمستشارون :**الأفراد أو الجهات الخارجية الذين يقدمون خدمات للمحافظة ويحتاجون إلى الوصول عن بعد إلى موارد تقنية محددة.
   - **الشركاء والموردون :**الشركاء التجاريون والموردون الذين يتطلب عملهم الوصول إلى بعض الأنظمة أو البيانات لتقديم الخدمات المتفق عليها.
2. **الموارد التقنية المشمولة:**
   - **الأنظمة الداخلية :**الأنظمة والتطبيقات الداخلية التي يمكن الوصول إليها عن بعد باستخدام شبكات آمنة مثل.VPN
   - **قواعد البيانات :**الوصول إلى قواعد البيانات الحساسة أو غير الحساسة التي تحتوي على معلومات المؤسسة.
   - **الخوادم والمخازن السحابية :**الوصول إلى الخوادم المحلية أو السحابية التي تستضيف تطبيقات المحافظة وبياناتها.
   - **أدوات التعاون والاتصال :**منصات الاتصال والتعاون مثل البريد الإلكتروني، أدوات الدردشة، وأدوات إدارة المشاريع.
3. **البيئات الداعمة:**
   - **الأجهزة الشخصية والمحمولة :**أجهزة الكمبيوتر المحمولة والهواتف الذكية والأجهزة اللوحية المستخدمة للوصول عن بعد إلى موارد المحافظة.

- **الشبكات المنزلية والعامة :**الشبكات التي يستخدمها الموظفون للوصول عن بعد، بما في ذلك الشبكات المنزلية والشبكات العامة (مع التنبيه على تجنب الأخيرة أو استخدام تدابير أمان إضافية).

هذا الدليل ملزم لجميع الأفراد والجهات التي تتعامل مع موارد المحافظة التقنية عن بعد، ويجب على الجميع الالتزام بالسياسات والإجراءات المنصوص عليها لضمان حماية الأنظمة والبيانات الخاصة بالمحافظة.

متطلبات الوصول عن بعد

لضمان الوصول الآمن والفعال إلى موارد المؤسسة التقنية من خارج بيئة العمل التقليدية، يتعين على المستخدمين الامتثال لمجموعة من المتطلبات التقنية والأمنية. وتتمثل هذه المتطلبات فيما يلي:

1. **الأجهزة المعتمدة**

- **الأجهزة الشخصية والمحمولة :**يجب أن تكون الأجهزة المستخدمة للوصول عن بعد، مثل أجهزة الكمبيوتر المحمولة أو الأجهزة اللوحية أو الهواتف الذكية، معتمدة من قبل دائرة تقنية المعلومات في المحافظة. ويجب أن تكون هذه الأجهزة مزودة بأحدث أنظمة التشغيل وتحديثات الأمان.
- **مواصفات الحد الأدنى :**يجب أن تستوفي الأجهزة المستخدمة للوصول عن بعد المواصفات التقنية المحددة من قبل الدائرة، والتي تشمل سرعة المعالج، ذاكرة الوصول العشوائي(RAM) ، وسعة التخزين.

2. **نظام التشغيل**

- **أنظمة التشغيل المدعومة :**يجب أن تكون الأجهزة التي تستخدم للوصول عن بعد تعمل بأنظمة تشغيل مدعومة، مثل Windows 10 أو أعلى، macOSالإصدار الأحدث، أو توزيعات Linux المعتمدة من المحافظة.
- **التحديثات الأمنية :**يتعين على المستخدمين التأكد من أن أنظمة التشغيل الخاصة بهم محدثة بأحدث التحديثات الأمنية لمنع أي ثغرات محتملة.

3. **البرامج المطلوبة**

- **برامج) VPN الشبكات الافتراضية الخاصة :(**يجب على المستخدمين تثبيت وتكوين برامج VPN المعتمدة من المحافظة للوصول الآمن إلى الشبكة الداخلية.
- **برامج مكافحة الفيروسات :**يجب أن تكون الأجهزة المستخدمة محمية ببرامج مكافحة الفيروسات المعتمدة وأن يتم تحديثها بانتظام لضمان الحماية من البرمجيات الخبيثة.

4. **التحقق من الهوية**

- **التحقق الثنائي :(Two-Factor Authentication)** يجب تمكين واستخدام التحقق الثنائي لكل محاولات الوصول عن بعد لتعزيز أمان الحسابات. يتضمن ذلك استخدام رموز التحقق المرسلة عبر الهاتف المحمول أو تطبيقات المصادقة.
- **إدارة كلمات المرور :**يجب استخدام كلمات مرور قوية وفريدة للوصول إلى الموارد التقنية، ويُفضل استخدام مديري كلمات المرور لإدارة كلمات المرور بأمان.

5. **حماية البيانات**

- **التشفير :**يجب تشفير جميع البيانات المنقولة بين الجهاز المستخدم والموارد التقنية التابعة للمؤسسة باستخدام بروتوكولات التشفير المعتمدة) مثل.(SSL/TLS
- **النسخ الاحتياطي :**يجب على المستخدمين التأكد من وجود نسخ احتياطية منتظمة للبيانات الهامة المخزنة على الأجهزة الشخصية، وذلك وفقًا لسياسات المؤسسة.

6. **الاستخدام الآمن للشبكات**

- **تجنب الشبكات العامة :**يجب الامتناع عن استخدام الشبكات العامة غير المؤمنة للوصول إلى موارد المؤسسة. في حالة الضرورة، يجب استخدام VPN لضمان تشفير الاتصال.
- **الشبكات المنزلية :**يُنصح المستخدمون بتأمين شبكاتهم المنزلية من خلال استخدام كلمات مرور قوية للشبكة وتحديث إعدادات الأمان الخاصة بجهاز التوجيه.(Router)

7. **الموافقات والتصاريح**

- **الموافقة المسبقة :**يجب الحصول على الموافقات اللازمة من الإدارة التقنية في المؤسسة قبل إعداد أو تعديل أي من إعدادات الوصول عن بعد.
- **التصاريح المحددة :**يجب التأكد من أن التصاريح الممنوحة للمستخدمين للوصول إلى الموارد التقنية عن بعد تتناسب مع احتياجاتهم الوظيفية ولا تتجاوزها.

8. **مراجعة وتحديث المتطلبات**

- **مراجعة دورية :**سيتم مراجعة هذه المتطلبات وتحديثها بانتظام لضمان مواكبتها للتطورات التكنولوجية وأحدث معايير الأمان.
- **إشعارات التحديث :**سيتم إخطار المستخدمين بأي تغييرات أو تحديثات في متطلبات الوصول عن بعد عبر القنوات المعتمدة داخل المؤسسة.

يهدف الالتزام بهذه المتطلبات إلى حماية موارد المحافظة التقنية وضمان استمرارية الأعمال بأمان وكفاءة عند العمل عن بعد.

السياسات والإجراءات

يهدف هذا القسم إلى توضيح السياسات والإجراءات التي يجب على جميع المستخدمين اتباعها عند الوصول عن بعد إلى الموارد التقنية للمؤسسة. هذه السياسات تهدف إلى حماية الأصول الرقمية وضمان الامتثال لمعايير الأمان والخصوصية.

1. **سياسة الاستخدام المقبول**

- **التزام المستخدم :**يجب على جميع المستخدمين الالتزام بسياسة الاستخدام المقبول عند الوصول إلى موارد المحافظة عن بعد. ويشمل ذلك استخدام الموارد التقنية فقط للأغراض المتعلقة بالعمل وعدم استخدام الأنظمة لأغراض شخصية أو غير قانونية.
- **حظر الأنشطة غير القانونية :**يمنع منعًا باتًا استخدام الأنظمة للوصول إلى أو توزيع محتوى غير قانوني أو ضار، بما في ذلك البرامج الضارة أو البريد المزعج.(Spam)
- **الاستخدام الأخلاقي للموارد :**يجب على المستخدمين استخدام الموارد التقنية بطرق تحترم حقوق الآخرين وتدعم بيئة عمل آمنة ومهنية.

2. **سياسة الأمان**

- **الحفاظ على سرية المعلومات :**يجب على المستخدمين ضمان حماية سرية المعلومات التي يتم الوصول إليها عن بعد وعدم مشاركتها مع أطراف غير مصرح لها.
- **إدارة كلمات المرور :**يجب استخدام كلمات مرور قوية وفريدة، وتغييرها بانتظام، والامتناع عن مشاركتها مع أي شخص آخر.
- **التحقق الثنائي :**يُفرض استخدام التحقق الثنائي (2FA) لجميع محاولات الوصول عن بعد لتعزيز أمان الحسابات.

3. **سياسة التحديث والصيانة**

- **التحديثات الدورية :**يجب على المستخدمين ضمان تحديث أنظمة التشغيل وبرامج الحماية بانتظام وفقًا لتوصيات قسم تقنية المعلومات.
- **الصيانة الوقائية :**يجب على المستخدمين الالتزام بعمليات الصيانة الوقائية للأجهزة والبرامج المستخدمة في الوصول عن بعد، بما في ذلك فحص الفيروسات وإصلاح الأخطاء.

4. **سياسة مراقبة النشاط**

- **مراقبة الوصول :**تحتفظ المؤسسة بحق مراقبة جميع الأنشطة التي تتم عبر الوصول عن بعد لضمان الامتثال للسياسات الأمنية ومنع أي نشاط غير مشروع.
- **التدقيق الدوري :**سيقوم قسم تقنية المعلومات بإجراء عمليات تدقيق دورية على الأنظمة لرصد أي محاولات اختراق أو نشاط غير معتاد.

5. **إجراءات الطوارئ**

- **الإبلاغ عن الحوادث :**يجب على المستخدمين الإبلاغ فورًا عن أي حوادث أمنية أو خروقات محتملة، مثل فقدان الأجهزة أو تسرب البيانات.

- **استجابة الطوارئ :**في حالة حدوث خرق أمني، يجب على المستخدمين اتباع خطة ادارة المخاطر التي تم وضعها من قبل المحافظة، والتي تشمل فصل الأجهزة المصابة وإبلاغ الدعم الفني.
- **استعادة الوصول :**سيتم توفير تعليمات محددة لاستعادة الوصول إلى الموارد في حال فقدانه بسبب مشكلات تقنية أو أمنية.

6. **الامتثال والتنفيذ**

- **التدريب والتوعية :**يجب على جميع المستخدمين حضور الدورات التدريبية المطلوبة المتعلقة بالوصول عن بعد وسياسات الأمان.
- **إجراءات التأديب :**سيتم اتخاذ إجراءات تأديبية في حالة عدم الامتثال للسياسات والإجراءات، والتي قد تتضمن تحذيرات، تعليق الوصول، أو اتخاذ إجراءات قانونية إذا لزم الأمر.
- **مراجعة السياسات :**سيتم مراجعة وتحديث السياسات والإجراءات بشكل دوري لضمان توافقها مع أحدث التهديدات الأمنية والتطورات التقنية.

7. **سياسة إدارة التحديثات**

- **التحديثات الأمنية :**يجب أن يقوم قسم تقنية المعلومات بإصدار تحديثات أمنية بشكل دوري للأجهزة والبرامج المستخدمة في الوصول عن بعد.
- **التحديثات الإلزامية :**في حالة إصدار تحديثات أمنية إلزامية، يجب على المستخدمين تثبيتها فورًا لضمان استمرارية الحماية.
- **الإشعارات :**سيتم إخطار المستخدمين بالتحديثات الهامة من خلال البريد الإلكتروني أو النظام الداخلي للمؤسسة.

يعتبر الالتزام بهذه السياسات والإجراءات جزءًا أساسيًا من الحفاظ على أمان وسلامة الأنظمة والبيانات الخاصة بالمحافظة. وتعد هذه السياسات ملزمة لجميع المستخدمين، ويجب مراجعتها وفهمها بعناية لضمان الامتثال الكامل.

إرشادات الدعم الفني

تُعتبر إرشادات الدعم الفني عنصرًا حيويًا لضمان حل المشكلات التقنية بفعالية وسرعة عند الوصول عن بعد إلى الموارد التقنية للمؤسسة. يهدف هذا القسم إلى توضيح كيفية الحصول على الدعم الفني، والقنوات المتاحة للتواصل، والإجراءات المتبعة لحل المشكلات.

1. **قنوات الدعم الفني**

- **البريد الإلكتروني للدعم الفني :**يمكن للمستخدمين إرسال طلبات الدعم الفني عبر البريد الإلكتروني المخصص للدعم. يجب أن يتضمن البريد الإلكتروني تفاصيل المشكلة، نوع الجهاز، وإجراءات الحل التي تم تجربتها بالفعل.
- **نظام التذاكر :**يُنصح باستخدام نظام التذاكر الإلكتروني إذا كان متاحًا، حيث يمكن للمستخدمين تسجيل طلبات الدعم ومتابعتها عبر منصة مخصصة.
- **الهاتف :**يمكن الاتصال بفريق الدعم الفني عبر الهاتف للحالات العاجلة التي تتطلب استجابة سريعة. يجب التأكد من توافر معلومات المستخدم الأساسية عند الاتصال.

2. **معلومات مهمة عند تقديم طلب دعم**

- **تفاصيل المشكلة :**يجب توضيح المشكلة أو الخطأ بأكبر قدر من الدقة، بما في ذلك الرسائل الخطأ أو الأعراض التي تم ملاحظتها.
- **الخطوات المتخذة :**توضيح أي خطوات تم اتخاذها لحل المشكلة بنفسك، مثل إعادة تشغيل الجهاز أو محاولة الاتصال مرة أخرى.
- **تفاصيل النظام :**تقديم تفاصيل حول النظام المستخدم، مثل نظام التشغيل، إصدار البرامج، ونوع الجهاز.
- **مستوى الأولوية :**تحديد مدى urgency (أولوية) المشكلة، وتوضيح ما إذا كانت تؤثر على العمليات اليومية أو إذا كانت مشكلة بسيطة يمكن تأجيل حلها.

3. **إجراءات حل المشكلات**

- **التحقق الأولي :**قد يقوم فريق الدعم الفني بالتحقق من بعض الأساسيات أولاً، مثل التأكد من اتصال الإنترنت، والتحقق من تحديثات البرامج، وإعادة تشغيل الجهاز.
- **الإرشادات الموجهة :**قد يتم تزويد المستخدمين بإرشادات محددة لإصلاح المشكلة، مثل خطوات لتعديل الإعدادات أو إعادة تثبيت برنامج معين.
- **التحقق من الوصول :**في بعض الحالات، قد يحتاج فريق الدعم إلى التحقق من الوصول إلى النظام عن بعد لإجراء مزيد من الفحص. يجب على المستخدمين منح الإذن اللازم وتوفير تفاصيل الاتصال المطلوبة.

4. **معالجة المشكلات المعقدة**

- **التصعيد (escalations):** في حال كانت المشكلة معقدة أو تتطلب تدخلًا خاصًا، سيتم تصعيد الطلب إلى مستوى أعلى من الدعم الفني، مثل مهندسي الأنظمة أو خبراء التقنية المتخصصين.

- **التقارير والتوثيق :**قد يتطلب الأمر توثيق المشكلة والحل بشكل مفصل للتأكد من عدم تكرارها ولتحليلها لاحقًا لتحسين إجراءات الدعم.

5. **متابعة وتقييم**

- **متابعة الحالة :**بعد تقديم طلب الدعم، يجب متابعة حالة الطلب عبر القنوات المتاحة، مثل نظام التذاكر أو البريد الإلكتروني.
- **تقييم الأداء :**قد يُطلب من المستخدمين تقديم تقييم لرضاهم عن جودة الخدمة المقدمة بعد حل المشكلة. سيساعد هذا في تحسين جودة الدعم الفني المقدم.

6. **دعم المستخدمين البعيدين**

- **الاتصال المرئي :**في بعض الحالات، قد يتطلب حل المشكلة استخدام أدوات الاتصال المرئي لمشاركة الشاشة والتفاعل مع المستخدمين عن بعد.
- **الدعم عن بعد :**يمكن لفريق الدعم الفني استخدام أدوات التحكم عن بعد لمساعدة المستخدمين في حل المشكلات على أجهزتهم بشكل مباشر، شريطة الحصول على إذن مسبق من المستخدم.

7. **الإجراءات الطارئة**

- **التعامل مع الأعطال الكبيرة :**في حالة الأعطال الكبيرة التي تؤثر على عدد كبير من المستخدمين، سيتم اتباع إجراءات خاصة للتعامل معها، مثل إشعار المستخدمين بتوقعات زمنية للحل وتقديم حلول بديلة مؤقتة إذا لزم الأمر.
- **إجراءات الطوارئ :**ستتبع المؤسسة خطة استجابة للطوارئ لضمان التعامل مع المشكلات التقنية الكبيرة بسرعة وفعالية.

تضمن إرشادات الدعم الفني هذه تقديم مساعدة فعالة وسريعة للمستخدمين عند مواجهة مشكلات تقنية أثناء الوصول عن بعد، مما يعزز استمرارية العمل ويقلل من التوقفات غير المخطط لها.