الدليل الاسترشادي لضوابط استخدام تطبيقات الاتصال المرئي في محافظة مسندم

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

قائمة المحتويات:

تعريفات 2
مقدمة 4
نطاق الدليل 4
أهداف الدليل الاسترشادي 4
تطبيقات الاتصال المرئي المشمولة 5
المتطلبات الأمنية لاستخدام تطبيقات الاتصال المرئي 5
قواعد استخدام التطبيقات 6
ضوابط الحضور والاجتماعات 6
إجراءات الطوارئ والتعامل مع المخاطر 6
مسؤوليات المستخدمين 7
التحديثات والتدريب 7
الامتثال والتنفيذ 7

تعريفات

تطبيقات الاتصال المرئي:(Video Conferencing Applications) برامج أو منصات رقمية تتيح التواصل الفوري بين الأفراد أو المجموعات من خلال الفيديو والصوت والرسائل النصية. تشمل تطبيقات مثلZoom ، Microsoft Teams، Google Meet، وCisco Webex.

التحقق الثنائي:(2FA - Two-Factor Authentication) عملية أمان إضافية تتطلب من المستخدمين تقديم معلومات تحقق إضافية (مثل رمز يُرسل عبر الهاتف المحمول) بجانب إدخال اسم المستخدم وكلمة المرور، لتعزيز مستوى الأمان.

المضيف:(Host) الشخص المسؤول عن إعداد وإدارة الاجتماع المرئي. يكون لديه الصلاحيات للتحكم في المشاركين، ضبط إعدادات الأمان، وتسجيل الاجتماع إذا لزم الأمر.

المشارك:(Participant) أي شخص ينضم إلى اجتماع مرئي أو جلسة عبر تطبيق الاتصال المرئي. يكون له دور محدود في الاجتماع ما لم يمنحه المضيف صلاحيات إضافية.

الشبكة الافتراضية الخاصة:(VPN - Virtual Private Network) تقنية تتيح إنشاء اتصال مشفر وآمن عبر الإنترنت بين جهاز المستخدم وشبكة المحافظة، مما يضمن حماية المعلومات أثناء الاتصال.

تشفير من طرف إلى طرف:(End-to-End Encryption) آلية أمان تضمن تشفير البيانات أثناء انتقالها من المرسل إلى المستقبل بحيث لا يمكن لأي طرف ثالث (بما في ذلك مزودي الخدمة) الوصول إلى محتوى الاتصال.

كلمة مرور الاجتماع:(Meeting Password) رمز سري يتم تعيينه لاجتماع مرئي لمنع الوصول غير المصرح به، حيث يجب على المشاركين إدخال كلمة المرور للانضمام إلى الاجتماع.

تسجيل الاجتماع:(Meeting Recording) عملية تسجيل الصوت أو الفيديو أو كلاهما خلال اجتماع مرئي. يجب أن يتم ذلك فقط بعد الحصول على إذن مسبق من المشاركين.

السياسة الأمنية:(Security Policy) مجموعة من الضوابط والإرشادات التي تضعها المحافظة لضمان أمان استخدام تطبيقات الاتصال المرئي، والتي تشمل حماية البيانات، التحقق من الهويات، وضبط إعدادات الأمان.

الخرق الأمني:(Security Breach) حادثة يتم فيها الوصول غير المصرح به إلى النظام أو البيانات، أو أي انتهاك لأمان المعلومات أثناء استخدام تطبيقات الاتصال المرئي.

إدارة المخاطر:(Incident Management) العملية التي تتبعها المحافظة للاستجابة للحوادث الأمنية والتقنية، بما في ذلك تحليل الحادث واتخاذ الإجراءات اللازمة لمعالجته وتقليل تأثيره.

المعلومات الحساسة:(Sensitive Information) البيانات أو المعلومات التي تتطلب حماية خاصة نظراً لطبيعتها الحساسة، مثل المعلومات الشخصية، البيانات المالية، أو أي معلومات تتعلق بأسرار العمل.

الخصوصية:(Privacy) حق المشاركين في حماية معلوماتهم الشخصية والبيانات التي يتم مشاركتها أثناء الاجتماعات المرئية من الوصول أو الكشف غير المصرح به.

السياسة المقبولة للاستخدام:(Acceptable Use Policy) مجموعة القواعد التي توضح الاستخدام المسموح به لتطبيقات الاتصال المرئي، وتحدد الأنشطة غير المسموح بها، مثل استخدام الأنظمة لأغراض غير مهنية.

الإعدادات الافتراضية:(Default Settings) الإعدادات القياسية التي يتم تعيينها تلقائيًا لتطبيقات الاتصال المرئي عند إنشاء حساب أو بدء اجتماع، والتي قد تحتاج إلى تعديل لتعزيز الأمان أو تحسين الأداء.

مقدمة

تحرص دائرة تقنية المعلومات في محافظة مسندم على تطبيق أفضل الممارسات في مختلف المجالات المتعلقة بالتحول الرقمي، و عليه طورت الدائرة الدليل الاسترشادي لاستخدام الاتصال المرئي والمسموع للاجتماعات الافتراضية أخذا بالاعتبار ضوابط استخدام تطبيقات الاتصال المرئي في وحدات الجهاز الإداري للدولة و الذي تم اعداده من قبل وزارة النقل و الاتصالات و تقنية والذي يعد أداة تنظيمية مبنية على أفضل الممارسات الدولية، ويعتبر هذا الدليل أحد الأدوات المساهمة في رفع مستوى الوعي بقواعد ومتطلبات الاتصال المرئي والمسموع لعقد الاجتماعات الافتراضية التي تحد من التعرض المحتمل للأضرار التي قد تنجم عن الاستخدام غير المصرح به لموارد المحافظة والتي تشمل فقدان بيانات حساسة أو سرية، والأضرار التي قد تؤثر على سمعة المحافظة، أو قد تؤثر على أنظمتها الداخلية.

نطاق الدليل

يشمل هذا الدليل جميع الأفراد العاملين بالمحافظة، بما في ذلك الموظفين الدائمين، المتعاقدين، والشركاء الذين يستخدمون تطبيقات الاتصال المرئي لأغراض العمل. كما يغطي جميع الأنظمة والأدوات المستخدمة لإجراء الاجتماعات الافتراضية، المؤتمرات، والندوات عبر الإنترنت.

أهداف الدليل الاسترشادي

يهدف الدليل الاسترشادي لضوابط استخدام تطبيقات الاتصال المرئي في محافظة مسندم إلى تحقيق ما يلي:

1. المساهمة في توفير الأدوات اللازمة للاتصال المرئي والمسموع وذلك من خلال بيان المتطلبات الأساسية لتجهيز البنى التحتية اللازمة لذلك
2. الإسهام بشكل فعال في تحسين التعاون بين منسوبي الجهة الحكومية وزيادة الإنتاجية وتوفير الوقت وتخطي حواجز المكان وعوائق الحضور من خلال استخدام مميزات الاتصال المرئي والمسموع لعقد الاجتماعات الافتراضية
3. رفع معدل استخدام خاصية المحادثات الفورية ومشاركة المحتوى والوثائق وغيرها من المميزات التي تتضمنها تطبيقات الاتصال المرئي والمسموع

تطبيقات الاتصال المرئي المشمولة

Google Meet ZOOM Microsoft Teams

وأي تطبيقات اتصال مرئي أخرى معتمدة من قبل المؤسسة.

المتطلبات الأمنية لاستخدام تطبيقات الاتصال المرئي

1. التحقق من الهوية

- استخدام التحقق الثنائي :(2FA) يتعين على المستخدمين تفعيل خاصية التحقق الثنائي عند تسجيل الدخول إلى تطبيقات الاتصال المرئي لضمان أمان الحسابات.
- المصادقة باستخدام البريد الإلكتروني المؤسسي :يجب على جميع المستخدمين استخدام بريدهم الإلكتروني المؤسسي عند التسجيل أو الدخول إلى تطبيقات الاتصال المرئي.

2. تشفير البيانات

- استخدام التشفير :يجب التأكد من أن تطبيق الاتصال المرئي يدعم التشفير من طرف إلى طرف (End-to-End Encryption) لحماية المحتوى المتبادل.
- حماية البيانات الحساسة :يجب الامتناع عن مشاركة أي بيانات حساسة أو معلومات سرية خلال الاجتماعات المرئية إلا إذا كان الاتصال مشفرًا بالكامل.

3. إعدادات الأمان

- قفل الاجتماع :بعد انضمام جميع المشاركين، يجب قفل الاجتماع لمنع أي دخول غير مصرح به.
- التحكم في المشاركين :يجب أن يكون لدى المضيف سيطرة كاملة على المشاركين، بما في ذلك القدرة على إزالة أي مشارك غير معروف أو غير مصرح له.
- استخدام كلمات مرور للاجتماعات :يجب دائمًا تعيين كلمة مرور لكل اجتماع، وتوزيعها فقط على المشاركين المعنيين.

قواعد استخدام التطبيقات

1. **الامتثال لسياسات الاستخدام المقبول**

يجب استخدام تطبيقات الاتصال المرئي فقط لأغراض العمل والاتصالات المتعلقة بالمهام المؤسسية. يُمنع استخدامها لأغراض شخصية أو غير مهنية أثناء ساعات العمل أو عبر الحسابات المؤسسية.

2. **حماية الخصوصية**

يجب على المستخدمين الالتزام بحماية خصوصية المشاركين الآخرين، وعدم تسجيل الاجتماعات أو مشاركة محتوياتها دون الحصول على موافقة مسبقة من جميع الأطراف المعنية.

3. **التحكم في المشاركة**

يجب على المضيفين ضبط الإعدادات بحيث لا يتمكن المشاركون من مشاركة الشاشة أو الملفات إلا بإذن مسبق، وذلك لتجنب أي مشاركة غير لائقة أو غير مخطط لها.

ضوابط الحضور والاجتماعات

1. **تسجيل الحضور**

- يتعين على المضيفين التأكد من أن جميع المشاركين في الاجتماع هم الأشخاص المصرح لهم بالحضور عبر التحقق من هويتهم قبل بدء الاجتماع.

2. **التسجيل والمشاركة**

- لا يجوز تسجيل الاجتماعات المرئية إلا بعد الحصول على إذن من المشاركين، ويجب إبلاغهم بوضوح في حال تم تفعيل ميزة التسجيل.
- يحق للمشاركين الامتناع عن استخدام الكاميرا أو الميكروفون إذا كان ذلك لا يؤثر على سير الاجتماع.

إجراءات الطوارئ والتعامل مع المخاطر

1. **التعامل مع الانتهاكات الأمنية**

- في حال تم اكتشاف أي انتهاك أمني أو محاولة اختراق أثناء اجتماع مرئي، يجب إنهاء الاجتماع فورًا، وإبلاغ قسم تقنية المعلومات لاتخاذ الإجراءات اللازمة.

2. **إدارة الحوادث**

- إذا حدثت مشكلة تقنية تعيق سير الاجتماع، يجب أن يكون هناك خطة بديلة، مثل الانتقال إلى تطبيق آخر أو تأجيل الاجتماع لحين حل المشكلة.

مسؤوليات المستخدمين

المضيف

يتحمل المضيف المسؤولية الكاملة عن إعدادات الاجتماع، بما في ذلك التحقق من هويات المشاركين، ضبط إعدادات الأمان، والتأكد من الالتزام بالسياسات المؤسسية

المشاركون

يجب على المشاركين احترام سياسات الاجتماع، الامتناع عن تسجيل أو مشاركة المحتوى دون إذن، والتعاون مع المضيف لضمان سير الاجتماع بشكل آمن وفعال.

التحديثات والتدريب

- **التدريب المستمر :**يجب أن يخضع جميع المستخدمين لتدريب دوري حول أحدث الممارسات الأمنية المتعلقة باستخدام تطبيقات الاتصال المرئي.
- **مراجعة التحديثات :**سيتم مراجعة وتحديث هذا الدليل بشكل دوري لتضمين أحدث المعايير والإرشادات الأمنية. سيتم إخطار المستخدمين بأي تغييرات جديدة.

الامتثال والتنفيذ

يعد هذا الدليل ملزمًا لجميع المستخدمين، ويجب الالتزام بجميع الضوابط والإرشادات الواردة فيه. قد يؤدي عدم الامتثال لهذه الإرشادات إلى اتخاذ إجراءات تأديبية بما يتناسب مع سياسة المحافظة.