هيئة تنظيم الاتصالات TRA
TELECOMMUNICATIONS REGULATORY AUTHORITY

إرشادات

إرشادات التعاون والعمل من المنزل لمدراء تقنية المعلومات

النسخة 1.1

تاريخ الإصدار: 19 مارس 2020

ص.ب. 26662، أبو ظبي، الإمارات العربية المتحدة
www.tra.gov.ae

جدول المحتويات

1. مقدمة

باتت الاجتماعات وأدوات التعاون الإلكترونية أدوات هامة لتسيير الأعمال اليومية في ضوء الجهود المبذولة لزيادة الإنتاجية والاستفادة من استثمارات تقنية المعلومات والاتصالات وخفض التكاليف وتقليل الوقت.

وهناك مجموعة متنوعة من الأدوات في السوق وتشمل خدمات الحوسبة السحابية المحلية.

الغرض من هذه الوثيقة التعريف بالجانب الأمني وإرشادات نشر واستخدام أدوات الاجتماعات والتعاون الإلكترونية عبر الإنترنت. وتعمل هذه الإرشادات على تعزيز مستوى أمان الأداة والثقة من استخدامها.

2. النطاق

تستهدف هذه الإرشادات جميع أفراد الجهات الحكومة الذين يستخدمون أدوات التعاون والعمل من المنزل مثل Mircrosoft Tram و Zoom و Cisco و Webex و Cisco Jabber وغيرها.

3. الإرشادات العامة للاستخدام التعاوني

هذه الإرشادات عامة وتنطبق على الحلول المحلية وحلول الخدمات السحابية.

يجب على الجهات إبلاغ من لديها من مستخدمين يعملون من المنزل بالتالي:

- عدم رفع أو مشاركة أي مرفق مهما كان دون فحص الملف للتأكد من خلوه من الفايروسات أو غيرها من البرمجيات الخبيثة.
- عدم استخدام أدوات التعاون الخاصة بالعمل لأي أغراض شخصية.
- عدم مشاركة الملفات من مصادر مجهولة.
- عدم قبول أي دعوة من مستخدمين مجهولين.
- الإبلاغ عن أي نشاط مشبوه لمدير النظام لديكم على الفور؛
- عدم تسجيل أو أخذ صور عن المحادثات من دون أخذ إذن جميع الأطراف وفقاً لسياسية مدير النظام/الجهة.
- بالنسبة للاجتماعات التي تتطلب تفعيل خاصية الكاميرا يرجى التأكد من اتباعكم قواعد الزي الرسمي.
- يجب على الموظفين الذين يستخدمون المنصات المتاحة الالتزام بسياسات الاستخدام المقبول والمعايير الأخلاقية وغير من السياسات المؤسسية للهيئة عند استخدام تلك المنصات.

- تعتبر المنصات قناة رسمية وينبغي استخدامها على هذا النحو. إن استخدام هذه المنصات لنشر الكراهية والمحتوى البذيء والألفاظ غير اللائقة سيتم إحالته لقسم الموارد البشرية وسيترتب عليه توجيه مخالفة أو تنبيه أو غيرها من تدابير أكثر صرامة بناءً على الحالة.
- يرجى العلم أن فريق الأمن والامتثال لديه القدرة على مراقبة الاستخدام لمنع انتشار المحتوى الضار مثل الفايروسات التي يمكن أن تضر ببيئة عمل تقنية المعلومات لدى الجهة.

4. إرشادات التعاون القائم على السحابة العامة

إذا نويتم استخدام الأدوات التعاونية القائمة على السحابة مثل مايكروسوفت تيمز، يتعين على المستخدمين معرفة الإرشادات الإضافية التالية:

- عدم مشاركة البيانات السرية عبر الصوت أو الوثائق أو الفيديو أو أي وسيلة اتصال أخرى.
- يمكن تشارك البيانات السرية فقط من خلال استخدام الحلول المحلية.

5. إرشادات مدراء الأنظمة على منصات محددة:

5.1. مايكروسوفت تيمز:

إذا نويتم استخدام مايكروسوفت تيمز، يجب أخذ الخطوات التالية بعين الاعتبار:

- عدم مزامنة Active Directory (الدليل النشط) الداخلي الخاص بكم مع ذلك الخاص بميكروسوفت أزور (Azure)؛
- التأكد من أن بيانات مؤسستكم تقع داخل دولة الإمارات. إذا كانت هذه رخصة جديدة ينبغي اختيار دولة الإمارات كمكان لإقامة البيانات. إذا كان هذا حساب قديم (قبل سنة 2019)، فقد تحتاجون إلى ترحيل بياناتكم ليصبح موقعها في دولة الإمارات.
- تفعيل خاصية المصادقة متعددة العوامل (Multi-Factor-Authentication) متى أمكن.
- تفعيل إمكانية إعادة ضبط كلمة المرور للموظفين للتقليل من جهود فريق الدعم.
- تحديد خطة Exchange Online للمستخدمين لإمكانية عرض تقويم الفريق.
- إخبار أعضاء فريقكم بعدم تبادل أي بيانات سرية عبر مشاركات الفريق.
- تقييد تسجيل جلسات الاجتماعات للأعضاء المخولين فقط.
- اقتصار المشاركات الرئيسية/العامة لفرق المؤسسة على الأعضاء المخولين فقط.
- تقييد وصول الضيوف إلى الفرق والقنوات الأخرى بمؤسستكم.
- تقييد عمليات إنشاء الفرق والقنوات لمسؤولي الفرق مع إغلاق خاصية MS Teams.

- مراقبة عمليات تسجيل دخول المستخدمين من الدليل النشط الخاص بأزور.

5.2. سيسكو جابر:

- تتم مصادقة الحساب من الدليل النشط فقط.
- تقييد الوصول إلى سيسكو جابر من خلال الشبكة الافتراضية الخاصة VPN
- إرشادات إضافية للاستخدام عبر شبكة الإنترنت بدون الاتصال بشبكة افتراضية خاصة.
  - لتفعيل الخدمة عبر الإنترنت (من دون شبكة افتراضية خاصة)، يجب عليكم اتباع إرشادات النشر الخاصة بسيسكو والوثائق عن أفضل الممارسات.
  - يجب توقيع شهادات الخادم بواسطة جهة إصدار شهادات موثوقة
  - استخدام البروتوكولات المشفرة مثل (https, srtp, srtcp)
  - التأكد من تسجيل عمليات الاتصال الواردة (مثلاً عن طريق syslog)
  - مراقبة/تسجيل (سجلات تفاصيل المكالمات) لرصد حالات إساءة الاستخدام.
- بالنسبة للاستخدام من الهاتف المتحرك، تقييد عنوان بروتوكول الإنترنت للوصول إلى الخادم واستخدام بيانات الاعتماد الممنوحة (مثال: السماح لعناوين بروتوكول الإنترنت من الدولة فقط للحد من مخاطر الهجمات من خارج الدولة)
- تثبيت سيسكو جابر من مستودع التطبيقات الداخلي.
- سحب جميع المستخدمين في مدير الاتصال من الدليل النشط بعد التكامل معه.
- القيام بتخصيص تحويلات أرقام الهاتف للمستخدمين في مدير الاتصال.

5.3. وبيبكس:

- دمج خدمة وبيبكس مع الدليل النشط بحيث يتم السماح بدخول المستخدمين المعتمدين فقط.
- سحب جميع المستخدمين من الدليل النشط بعد التكامل معه.
- تقديم خدمات وبيبكس الخارجية عند تفعيل شبكة DMZ التي تتميز بانفتاح أكبر من تلك المحلية.
- تقديم الخدمات المبنية على HTTPS فقط لخادم وبيبكس الخارجي مع معيار وحيد وهو وجود جدار حماية.

5.4. أفايا Workplace:

- دمج تطبيق Avaya Workplace مع الدليل النشط بحيث يتم السماح بدخول المستخدمين المعتمدين فقط.
- سحب جميع المستخدمين من الدليل النشط بعد التكامل معه.
- تقديم خدمات Avaya Workplace الخارجية عند تفعيل شبكة DMZ التي تتميز بانفتاح أكبر من تلك المحلية.
- تقديم الخدمات المبنية على HTTPS فقط لخادم Avaya Workplace الخارجي مع معيار وحيد وهو الانفتاح على شبكة الإنترنت.

6. عدم الامتثال:

هذه الإرشادات اختيارية ولكن قد ينتج عن عدم الامتثال مخاطر أمنية وقانونية ومالية لا داعي لها. وقد يشمل ذلك مخالفة قوانين الدولة وسياسات الهيئة ومعايير ضمان المعلومات وسياسات تقنية المعلومات والموارد البشرية الحكومية.