



الأكاديمية السلطانية للإدارة
ROYAL ACADEMY OF MANAGEMENT

ضوابط استخدام تطبيقات الاتصال المرئي

الصفحة

2
2
2
3
5
6
8
9

جدول المحتويات

1. المقدمة
2. الغرض
3. نطاق التطبيق
4. الضوابط العامة
5. ضوابط الحضور والمشاركة
6. ضوابط الأمن
7. المسؤوليات
8. الخلاصة

1. المقدمة

مع التطور السريع في تقنيات الاتصال وتوسع نطاق استخدام تطبيقات الاتصال المرئي في المؤسسات الحكومية، أصبحت هذه التطبيقات أداة أساسية لتعزيز التواصل الفعال بين مختلف الدوائر والأقسام، سواء على المستوى الداخلي أو الخارجي. تُمكن تطبيقات الاتصال المرئي من عقد الاجتماعات والمناقشات بشكل فوري وفعال، مما يساهم في تسريع عمليات اتخاذ القرار وتنسيق العمل بين الفرق المختلفة. ومع ذلك، يرافق هذا الاعتماد المتزايد على تقنيات الاتصال المرئي مجموعة من التحديات المتعلقة بأمن المعلومات، وسرية البيانات، وضمان الاستخدام الأمثل لهذه الأدوات. في ظل هذه التحديات، تبرز الحاجة إلى وضع ضوابط وإرشادات واضحة تنظم كيفية استخدام تطبيقات الاتصال المرئي داخل الأكاديمية السلطانية للإدارة، بما يضمن تحقيق أقصى استفادة من هذه التقنيات مع الحفاظ على أعلى مستويات الأمن والخصوصية. يهدف هذا المستند إلى تقديم إطار شامل للضوابط والإجراءات التي يجب اتباعها عند استخدام تطبيقات الاتصال المرئي في الأكاديمية. من خلال هذه الضوابط، تسعى الأكاديمية إلى تعزيز ثقافة الاستخدام الآمن لتلك التطبيقات، وضمان التزام جميع الموظفين والمتعاملين بالإجراءات المعتمدة، مما يساهم في حماية المعلومات الحكومية الحساسة وتحقيق التواصل الفعال بين جميع الأطراف المعنية.

2. الغرض

يهدف هذا المستند إلى توفير إطار عمل متكامل لتنظيم استخدام تطبيقات الاتصال المرئي داخل الأكاديمية، وذلك من خلال تحديد مجموعة من الضوابط والإجراءات التي تضمن الاستخدام الآمن والفعال لهذه التطبيقات. يسعى هذا الإطار إلى تحقيق التوازن بين الاستفادة القصوى من تقنيات الاتصال الحديثة وتعزيز الكفاءة التشغيلية للأكاديمية، وبين الحفاظ على سرية المعلومات وحمايتها من أي مخاطر أمنية. يتضمن هذا المستند أيضاً توجيهات واضحة تضمن الامتثال للسياسات الحكومية والأطر التنظيمية المتعلقة بحماية البيانات والخصوصية. كما يهدف إلى توعية جميع الموظفين والمتعاملين بأهمية اتباع أفضل الممارسات في استخدام تطبيقات الاتصال المرئي، مما يعزز من فعالية الاجتماعات الرقمية ويضمن تحقيق الأهداف المؤسسية بكفاءة وموثوقية. بشكل عام، يسعى هذا المستند إلى دعم الأكاديمية في استغلال الفرص التي توفرها تقنيات الاتصال المرئي، مع مراعاة جميع الجوانب الأمنية والتنظيمية، لضمان بيئة عمل آمنة ومنتجة تتماشى مع متطلبات العصر الرقمي.

3. نطاق التطبيق

يعد نطاق التطبيق جزءاً أساسياً في تنظيم وضبط استخدام تطبيقات الاتصال المرئي داخل الأكاديمية. الهدف من تحديد نطاق التطبيق هو توضيح الفئات والأدوار التي تنطبق عليها السياسات والإجراءات الموضحة في هذا المستند، بالإضافة إلى تحديد السياقات والأنشطة التي تشملها هذه السياسات. إن تحديد نطاق التطبيق يضمن أن جميع الأفراد والجهات المعنية على دراية كاملة بالمسؤوليات والضوابط التي يجب اتباعها عند استخدام تقنيات الاتصال المرئي، سواء كان ذلك في الاجتماعات الداخلية، أو عند التعامل مع أطراف خارجية، أو في حالات التعاون مع جهات متعددة. يمتد نطاق التطبيق ليشمل كافة مستويات الأكاديمية ويحدد بوضوح الفئات التي يتعين عليها الالتزام بهذه الإجراءات، مما يساعد على خلق بيئة عمل آمنة ومنظمة تساهم في تحقيق الأهداف المؤسسية بفعالية.



4. الضوابط العامة

تعتبر الضوابط العامة حجر الأساس لضمان الاستخدام الأمثل والأمن لتطبيقات الاتصال المرئي داخل الأكاديمية. تهدف هذه الضوابط إلى توجيه الموظفين والمتعاملين في كيفية استخدام هذه التطبيقات بشكل يتوافق مع سياسات الأكاديمية، مع مراعاة أعلى معايير الأمان والسرية. تتضمن الضوابط العامة مجموعة من الإرشادات والإجراءات التي تضمن حماية المعلومات، وضبط المشاركة الفعالة، والتأكد من استخدام التطبيقات المعتمدة بطريقة فعالة وأمنة. هذه الضوابط تساهم في تحسين تجربة الاجتماعات المرئية وضمان سيرها بطريقة منظمة وموثوقة. الالتزام بهذه الضوابط يساهم في حماية البيانات الحساسة من أي اختراقات أو تسريبات، ويعزز من كفاءة العمل الجماعي، ويضمن توافق العمليات اليومية مع المعايير الأمنية والتنظيمية المتبعة في الأكاديمية.

اختيار التطبيقات

- يجب استخدام تطبيقات الاتصال المرئي التي تم اعتمادها من قبل تقنية المعلومات في الأكاديمية. يتم اختيار هذه التطبيقات بناءً على معايير الأمان، الكفاءة، وسهولة الاستخدام.
- يمنع منعاً باتاً استخدام أي تطبيقات لم يتم اعتمادها رسمياً من قبل الأكاديمية. يهدف هذا الإجراء إلى الحد من المخاطر الأمنية وحماية بيانات الأكاديمية.

تحديث التطبيقات

- يجب على جميع المستخدمين التأكد من تحديث تطبيقات الاتصال المرئي إلى أحدث الإصدارات المتاحة بشكل دوري. تتضمن التحديثات عادةً تحسينات أمن وإصلاحات للأخطاء التي قد تؤثر على الأداء.
- في حالة إصدار تحديثات طارئة لمعالجة ثغرات أمنية أو مشاكل خطيرة، يتعين على المستخدمين تثبيت هذه التحديثات فوراً دون تأخير.

الدخول إلى الاجتماعات

- يجب على جميع الموظفين استخدام حسابات الأكاديمية الرسمية عند الانضمام إلى الاجتماعات المرئية. يمنع استخدام الحسابات الشخصية أو غير المعترف بها من قبل الأكاديمية
- يُنصح بتفعيل المصادقة الثنائية (Two-Factor Authentication) عند تسجيل الدخول إلى تطبيقات الاتصال المرئي

حماية البيانات

- يجب التأكد من أن جميع الاجتماعات المرئية مشفرة من البداية إلى النهاية (end-to-end encryption) لضمان حماية البيانات المتداولة
- يجب أن يتم تحديد المشاركين في الاجتماعات بعناية لضمان أن الوصول إلى المعلومات الحساسة يقتصر على الأشخاص المعنيين فقط
- يمنع تسجيل الاجتماعات أو التقاط صور للشاشات أو توثيقها بأي شكل من الأشكال دون الحصول على إذن مسبق من جميع المشاركين. عند الحاجة للتسجيل لأغراض رسمية، يجب اتباع السياسات والإجراءات المعتمدة

سرية المعلومات

- يجب التأكد من أن جميع المشاركين في الاجتماع لديهم الصلاحيات اللازمة للوصول إلى المعلومات التي سيتم مناقشتها
- يمنع مشاركة الملفات الحساسة أو السرية عبر تطبيقات الاتصال المرئي دون استخدام بروتوكولات التشفير المناسبة

بيئة الاجتماعات

- يجب عقد الاجتماعات في بيئة خالية من التشويش والضوضاء لضمان التركيز الكامل وحماية سرية المناقشات
- يجب على الموظفين التأكد من أن الأشخاص غير المعنيين لا يمكنهم الاستماع أو مشاهدة ما يجري في الاجتماع، خاصة عند عقد الاجتماعات من أماكن خارجية

إدارة المشاركين

- يجب على منظم الاجتماع التحكم لمن يُسمح له بالدخول والخروج من الاجتماع. ينصح باستخدام ميزات مثل غرف الانتظار (Waiting Rooms) للتحكم في انضمام المشاركين
- يجب مراقبة نشاط المشاركين خلال الاجتماع للتأكد من عدم وجود أي تصرفات غير ملائمة أو محاولات للوصول إلى معلومات غير مصرح بها

الامتثال للقوانين واللوائح

- يجب على جميع المستخدمين الالتزام بالسياسات الحكومية والقوانين المحلية والدولية المتعلقة بحماية البيانات والخصوصية عند استخدام تطبيقات الاتصال المرئي
- يجب على المستخدمين الموافقة على شروط استخدام التطبيقات وفقاً للسياسات المعتمدة من قبل الأكاديمية قبل استخدامها

الدعم التقني

- يجب على دائرة تقنية المعلومات توفير الدعم الفني المستمر للمستخدمين للتعامل مع أي مشاكل تقنية قد تطرأ أثناء استخدام تطبيقات الاتصال المرئي
- يتعين على الأكاديمية توفير برامج تدريبية وتوعوية للمستخدمين حول كيفية استخدام تطبيقات الاتصال المرئي بشكل آمن وفعال

5- ضوابط الحضور والمشاركة

تشكل ضوابط الحضور والمشاركة أساساً لضمان سير الاجتماعات المرئية بشكل فعال ومنظم داخل الأكاديمية. تهدف هذه الضوابط إلى تحديد كيفية تفاعل المشاركين في الاجتماعات المرئية، وضبط آلية الحضور والانضمام، إضافةً إلى توجيه أساليب التفاعل والمشاركة لتحقيق أقصى استفادة من هذه الاجتماعات. تساهم هذه الضوابط في خلق بيئة تواصل احترافية تحافظ على الانضباط، وتضمن الالتزام بجدول الأعمال، وتحقيق الأهداف المرجوة من الاجتماعات. كما تساعد في ضبط وقت الاجتماعات بشكل فعال، وتقليل التشويش والمقاطعات غير الضرورية، وتعزيز التركيز على المواضيع المطروحة. الالتزام بضوابط الحضور والمشاركة يعزز من مستوى التعاون بين الموظفين، ويحافظ على سلاسة الاجتماعات الرقمية، ويضمن احترام وقت وجهود جميع المشاركين.

الانضمام في الوقت المحدد

- على جميع المشاركين الانضمام إلى الاجتماع في الوقت المحدد. وعلى منظم الاجتماع التأكيد على أهمية الالتزام بالمواعيد لضمان سير الاجتماع بشكل سلس
- في حال تأخر أحد المشاركين عن موعد الاجتماع، يجب عليه الحصول على إذن مسبق من منظم الاجتماع قبل الانضمام. يمكن أن يتم وضع آلية تسمح بدخول المتأخرين دون تشويش على سير الاجتماع، مثل كتم الصوت عند الدخول تلقائياً

التحقق من الهوية

- على منظم الاجتماع التحقق من هوية جميع المشاركين قبل بدء الاجتماع. يمكن القيام بذلك من خلال إرسال دعوات محددة للمشاركين المعتمدين عبر البريد الإلكتروني الرسمي أو باستخدام تقنيات المصادقة الثنائية
- على جميع المشاركين استخدام أسمائهم الرسمية كما هي مسجلة في الأكاديمية عند الدخول إلى الاجتماع. يمنع استخدام الألقاب أو الأسماء المستعارة

التفاعل والمشاركة الفعّالة

- على جميع المشاركين التفاعل مع محتوى الاجتماع والمشاركة بأفكارهم وملاحظاتهم بشكل مهني ومناسب. يُشجع على طرح الأسئلة والمساهمة في النقاشات، ولكن بشكل منظم ووفقاً لدور كل مشارك
- على المشاركين استخدام الميزات المتاحة في تطبيقات الاتصال المرئي بشكل صحيح، مثل رفع اليد الافتراضية (Raise Hand) لطلب الكلمة، واستخدام الدردشة (Chat) للتواصل الجانبي أو تقديم ملاحظات سريعة دون مقاطعة المتحدث

الالتزام بالأجندة

- على المشاركين مراجعة جدول الأعمال (الأجندة) وتحضير الملاحظات والأسئلة المتعلقة بالمواضيع المدرجة قبل بدء الاجتماع. يساهم ذلك في تحسين جودة النقاش وتوفير الوقت
- على المشاركين الالتزام بجدول الأعمال المحدد وعدم طرح مواضيع خارجة عن نطاق الاجتماع إلا إذا تم الاتفاق على ذلك مسبقاً. يجب أن يتحكم منظم الاجتماع في إدارة الوقت وتوجيه النقاشات لضمان التزام الجميع بالأجندة

استخدام الصوت والفيديو

- يجب على المشاركين كتم الصوت (Mute) عندما لا يكونون متحدثين لتجنب التشويش على الآخرين. يساعد هذا في الحفاظ على وضوح الصوت ومنع الضوضاء غير الضرورية
- في الاجتماعات الرسمية أو عند طلب منظم الاجتماع، يُفضل تشغيل الكاميرا لضمان التفاعل الشخصي. ومع ذلك، يجب أن يختار المشاركون خلفية مناسبة خالية من المشتتات

إدارة الوقت

- على منظم الاجتماع التأكد من أن كل بند في الأجندة يُناقش ضمن الوقت المحدد له، وتوجيه النقاشات لإنهائها في الوقت المحدد
- إذا ظهرت مواضيع إضافية غير مدرجة في الأجندة وتطلبت نقاشاً، يجب على منظم الاجتماع تخصيص وقت محدد لها في نهاية الاجتماع أو تأجيلها للاجتماع القادم

الاحترام المهني

- يجب على جميع المشاركين الالتزام بأعلى معايير الاحترام المهني أثناء الاجتماع، سواء في التحدث أو الاستماع للآخرين. يمنع استخدام لغة غير لائقة أو السخرية من آراء الآخرين
- يُنصح المشاركون بالتركيز الكامل على الاجتماع وتجنب الانشغال بأنشطة أخرى مثل استخدام الهاتف الشخصي أو إرسال رسائل بريد إلكتروني خلال وقت الاجتماع

التعامل مع الأعطال التقنية

- في حالة حدوث أي مشكلة تقنية تؤثر على قدرة أحد المشاركين على الانضمام إلى الاجتماع أو التفاعل معه، يجب عليه إبلاغ منظم الاجتماع فوراً عبر وسائل الاتصال البديلة (مثل البريد الإلكتروني أو الهاتف)
- يُنصح بأن يكون لدى المشاركين خطة احتياطية في حالة تعطل الاتصال المرئي، مثل الانتقال إلى جهاز آخر أو استخدام اتصال إنترنت بديل

مغادرة الاجتماع

- إذا كان على أحد المشاركين مغادرة الاجتماع قبل انتهائه، يجب عليه إبلاغ منظم الاجتماع مسبقاً وتقديم اعتذار بسيط دون مقاطعة سير الاجتماع
- يجب على منظم الاجتماع الإعلان عن انتهاء الاجتماع بشكل رسمي وشكر المشاركين على حضورهم وتفاعلهم قبل إنهاء الاتصال

6. ضوابط الأمن

تعتبر ضوابط الأمن العنصر الأكثر أهمية عند استخدام تطبيقات الاتصال المرئي في الأكاديمية، حيث تهدف هذه الضوابط إلى حماية المعلومات الحساسة وضمان سرية الاجتماعات من أي تهديدات أمنية محتملة. مع تزايد الاعتماد على تقنيات الاتصال المرئي، تزداد أهمية تبني تدابير أمنية قوية تمنع الوصول غير المصرح به إلى البيانات، وتحد من المخاطر المرتبطة بالاختراقات والتسريبات. تشمل ضوابط الأمن مجموعة من الإجراءات التي تضمن تأمين بيئة الاجتماعات الافتراضية، مثل استخدام التشفير، إدارة صلاحيات المشاركين، وتفعيل إعدادات الأمان المتاحة في التطبيقات المستخدمة. هذه الضوابط ضرورية لضمان حماية المعلومات المتداولة، سواء كانت داخل الأكاديمية أو في التعامل مع جهات خارجية. الالتزام بضوابط الأمن يعزز من ثقة الأكاديمية في استخدام تقنيات الاتصال المرئي ويوفر حماية مستدامة لبياناتها، مما يضمن استمرار العمليات بشكل آمن وفعال دون تعريض المعلومات لأي مخاطر غير ضرورية.

إعدادات الأمن الأساسية

- يجب التأكد من تفعيل التشفير الكامل (End-to-End Encryption) في جميع الاجتماعات المرئية لضمان حماية المعلومات المتداولة من أي اختراقات أو اعتراضات
- يجب تعيين كلمة مرور لكل اجتماع مرئي لضمان أن المشاركين المصرح لهم فقط هم من يمكنهم الانضمام. يتم توزيع كلمات المرور عبر قنوات آمنة ويجب تحديثها بانتظام

إدارة المشاركين

- يُنصح باستخدام ميزة غرف الانتظار (Waiting Rooms) التي تسمح لمنظم الاجتماع بالتحكم لمن يمكنه الدخول إلى الاجتماع، وذلك للتأكد من أن المشاركين المصرح لهم فقط يمكنهم الانضمام
- قبل السماح لأي شخص بالدخول إلى الاجتماع، يجب على منظم الاجتماع التحقق من هويته والتأكد من أنه مصرح له بالمشاركة. يمكن استخدام تقنيات التحقق المزدوجة لهذا الغرض



التحكم في الميزات المتاحة للمشاركين

- يجب على منظم الاجتماع تحديد صلاحيات المشاركين بعناية، مثل التحكم لمن يمكنه مشاركة الشاشة أو التحدث أو استخدام الدردشة. ينصح بتحديد صلاحيات معينة لكل مشارك حسب دوره في الاجتماع
- يجب تعطيل خيار التسجيل لجميع المشاركين إلا بإذن منظم الاجتماع. إذا كان التسجيل ضرورياً، يجب إعلام جميع المشاركين بذلك والحصول على موافقتهم المسبقة



حماية المعلومات المتداولة

- ينبغي عدم مشاركة المعلومات الحساسة أو السرية عبر تطبيقات الاتصال المرئي إلا إذا كانت هناك حاجة ماسة لذلك. في حالة الضرورة، يجب التأكد من أن المعلومات مشفرة بشكل كافٍ
- يجب استخدام بروتوكولات آمنة مثل SSL/TLS عند نقل الملفات أو المعلومات الحساسة خلال الاجتماع. يفضل استخدام منصات مشاركة ملفات مشفرة ومعتمدة بدلاً من إرسالها عبر الدردشة في تطبيقات الاتصال المرئي



التحديات الأمنية

- يجب التأكد من تحديث تطبيقات الاتصال المرئي بشكل منتظم لضمان الحصول على أحدث تصحيحات الأمن. يشمل ذلك التطبيقات المثبتة على أجهزة المستخدمين والبنية التحتية الخلفية
- ينبغي على دائرة تقنية المعلومات مراجعة وتحديث إعدادات الأمن الخاصة بتطبيقات الاتصال المرئي بانتظام، لضمان مواكبة التهديدات الأمنية الجديدة



إجراءات التعامل مع الحوادث الأمنية

- في حالة اكتشاف أي خرق أمني أو محاولة اختراق أثناء استخدام تطبيقات الاتصال المرئي، يجب على المستخدمين الإبلاغ فوراً إلى دائرة تقنية المعلومات بالأكاديمية
- يجب أن يكون لدى الأكاديمية خطة استجابة لحالات الطوارئ تتضمن إجراءات فورية للتعامل مع الخروقات الأمنية، مثل إغلاق الاجتماعات المشبوهة، إلغاء صلاحيات الوصول، وتغيير كلمات المرور



التأمين من بيئة العمل

- يجب عقد الاجتماعات المرئية في بيئة آمنة وخالية من التداخلات الخارجية. في حالة العمل من المنزل أو من مكان خارجي، ينبغي التأكد من أن الأشخاص غير المعنيين لا يمكنهم الاستماع إلى الاجتماع أو مشاهدة المحتوى
- يُنصح باستخدام الأجهزة المعتمدة من قبل الأكاديمية فقط لعقد الاجتماعات المرئية. هذه الأجهزة يجب أن تكون مؤمنة بشكل كافٍ وتتضمن برمجيات الحماية اللازمة



مراجعة وضبط الأمن بشكل دوري

- يجب على الأكاديمية مراجعة سياسات الأمن الخاصة باستخدام تطبيقات الاتصال المرئي بشكل دوري، وتحديثها بناءً على التغيرات في البيئة التقنية أو التهديدات الأمنية
- يُنصح بإجراء اختبارات دورية على إعدادات الأمن لتطبيقات الاتصال المرئي، مثل اختبارات الاختراق (Penetration Testing) لضمان عدم وجود ثغرات أمنية





تعد المسؤولية والأدوار جزءاً حيوياً في تنظيم وضمان الاستخدام الفعال والأمن لتطبيقات الاتصال المرئي داخل الأكاديمية. إن تحديد المسؤولية بوضوح يساهم في توزيع المهام بين مختلف الأفراد والفرق المعنية، مما يساعد على تجنب الفوضى أو تضارب الأدوار، ويضمن تطبيق السياسات والإجراءات بشكل فعال.

كل دور داخل الأكاديمية، من دائرة تقنية المعلومات إلى منظمي الاجتماعات والموظفين العاديين، يتحمل مسؤولية محددة تتعلق باستخدام تطبيقات الاتصال المرئي. يتضمن ذلك مسؤوليات تتعلق بتأمين البيانات، إدارة المشاركين، مراقبة الأنشطة، والإبلاغ عن أي حوادث أمنية أو تقنية. تحديد الأدوار والمسؤوليات يساهم في خلق بيئة عمل منظمة ومسؤولة، حيث يعرف كل فرد دوره ويعمل ضمن إطار محدد لضمان حماية المعلومات وتعزيز الكفاءة في الاجتماعات المرئية. الالتزام بهذه الأدوار يعزز من كفاءة العمل الجماعي ويساهم في تحقيق أهداف الأكاديمية بفعالية.

توزيع المسؤولية بشكل واضح يساعد على ضمان الالتزام بضوابط استخدام تطبيقات الاتصال المرئي، ويضمن استعداد جميع الأطراف المعنية للتعامل مع أي تحديات قد تنشأ. فيما يلي توضيح تفصيلي للمسؤوليات المختلفة:



دائرة تقنية المعلومات

- اختيار واعتماد تطبيقات الاتصال المرئي المستخدمة داخل الأكاديمية بناءً على معايير الأمن، الكفاءة، وسهولة الاستخدام. يجب أن تضمن الإدارة أن هذه التطبيقات تلبّي جميع متطلبات الأمن وأنها متوافقة مع السياسات الحكومية
- متابعة تحديثات التطبيقات بشكل دوري وتوفير الدعم الفني المستمر لضمان عدم وجود ثغرات أمنية. كما يجب عليها إدارة إعدادات الأمن العامة للتطبيقات ومراقبة استخدامها
- تقديم الدعم الفني لجميع المستخدمين داخل الأكاديمية للتعامل مع المشاكل التقنية التي قد تواجههم أثناء استخدام تطبيقات الاتصال المرئي، بما في ذلك الإعدادات الأولية وإجراءات الأمن
- توفير برامج تدريبية وتوعوية للموظفين حول كيفية استخدام التطبيقات بشكل آمن وفعال، بالإضافة إلى توعيتهم بأحدث التهديدات الأمنية وكيفية التعامل معها



منظمو الاجتماعات

- مسؤولون عن إعداد الاجتماعات المرئية، بما في ذلك تحديد قائمة المشاركين، توزيع الدعوات، وضمان أن جميع المشاركين يستخدمون حسابات معتمدة من الأكاديمية
- التأكد من تفعيل جميع إعدادات الأمن اللازمة، مثل التحقق من هوية المشاركين، استخدام غرف الانتظار، وتفعيل التشفير
- إدارة دخول وخروج المشاركين من الاجتماع، وضبط صلاحياتهم خلال الاجتماع، مثل التحكم فيمن يمكنه مشاركة الشاشة أو استخدام الدردشة
- اتخاذ القرارات الفورية لتعليق الاجتماع أو إنهائه في حالة حدوث خرق أمني أو مشكلة تقنية كبيرة، وإبلاغ دائرة تقنية المعلومات بشكل فوري



جميع الموظفين والمستخدمين

- ملزمون بالالتزام بالسياسات والإجراءات المحددة في هذا المستند، بما في ذلك استخدام التطبيقات المعتمدة، والحفاظ على سرية المعلومات، وتطبيق إجراءات الأمن
- التأكد من أن المعلومات المتداولة خلال الاجتماعات المرئية تظل سرية، وعدم مشاركة أي معلومات حساسة إلا وفقاً للسياسات المعتمدة
- الإبلاغ فوراً عن أي حوادث أمنية أو مشكلات تقنية تطرأ أثناء استخدام تطبيقات الاتصال المرئي إلى منظم الاجتماع أو دائرة تقنية المعلومات
- الالتزام بالمشاركة الفعالة في الاجتماعات وفقاً للضوابط المحددة، بما في ذلك الالتزام بأجندة الاجتماع، احترام المواعيد، والحفاظ على مستوى مهني عالٍ في التفاعل مع الزملاء



الإدارة العليا

- اعتماد السياسات والإجراءات المتعلقة باستخدام تطبيقات الاتصال المرئي، وضمان توافقها مع الأهداف الاستراتيجية للأكاديمية
- مراقبة الالتزام بالسياسات والإجراءات المعتمدة من خلال تقارير دورية وعمليات تدقيق داخلية، واتخاذ الإجراءات التصحيحية عند الضرورة
- توفير الدعم الكافي للمبادرات الأمنية والتقنية التي تطلقها دائرة تقنية المعلومات، بما في ذلك توفير الموارد اللازمة وتوجيه التوجيهات الاستراتيجية



قسم أمن المعلومات

- مراقبة الأنشطة داخل تطبيقات الاتصال المرئي للكشف عن أي محاولات اختراق أو نشاط غير عادي قد يشير إلى تهديد أمني
- عند حدوث خرق أمني، يكون فريق أمن المعلومات مسؤول عن تحليل الحادث وتحديد كيفية حدوثه، وتقديم توصيات لتجنب تكرار الحادث في المستقبل
- مراجعة وتحديث بروتوكولات الأمن بشكل دوري لضمان مواكبتها لأحدث التهديدات والتقنيات المتاحة



الجهات الخارجية والمتعاقدون

- يجب على الجهات الخارجية والمتعاقدين الذين يستخدمون تطبيقات الاتصال المرئي الخاصة بالأكاديمية الالتزام بجميع الضوابط الأمنية والإجراءات المنصوص عليها في هذا المستند
- يجب عليهم التعامل مع المعلومات التي يتم تبادلها خلال الاجتماعات المرئية بسرية تامة، وتجنب مشاركة هذه المعلومات مع أطراف أخرى دون إذن صريح من الأكاديمية
- يتعين على الجهات الخارجية والمتعاقدين التعاون الكامل مع دائرة تقنية المعلومات في حالة حدوث أي مشكلة تقنية أو خرق أمني، بما في ذلك الالتزام بالإجراءات الطارئة المتخذة

8. الخلاصة

إن استخدام تطبيقات الاتصال المرئي في الأكاديمية السلطانية لإدارة يوفر فرصاً كبيرة لتعزيز التواصل الفعال وتحقيق الكفاءة في العمل. ومع ذلك، فإن هذا الاستخدام يجب أن يكون محكوماً بضوابط وإجراءات تضمن حماية المعلومات والبيانات الحساسة وضمان سرية الاجتماعات والمناقشات. هذا المستند يحدد مجموعة من الضوابط والإرشادات التي تهدف إلى تنظيم استخدام هذه التطبيقات داخل الأكاديمية، والتي ينبغي على جميع الموظفين والمتعاملين الالتزام بها.

إن الالتزام بهذه الضوابط لا يعزز فقط أمن المعلومات وسرية البيانات، ولكنه أيضاً يعكس مدى احترافية الأكاديمية واهتمامها بتبني أفضل الممارسات في إدارة عملياتها.

ختاماً، ينبغي على جميع الأطراف ذات العلاقة مراجعة هذه الضوابط بشكل دوري والتأكد من تطبيقها بشكل صحيح، مع مراعاة التحديثات المستمرة لتقنيات الاتصال لضمان بقاء الأكاديمية في مقدمة الجهات التي تتبنى الحلول التقنية الحديثة بشكل آمن وفعال.