

تأمين أنظمة الاجتماعات عن بعد

يمكن تأمين بيئة عمل الاجتماعات عن بعد من خلال اتباع الإرشادات التالية:

يجب التأكد من

- 1 تحديث البرنامج أو التطبيق الخاص بالاجتماع عن بعد وفقاً للتحديثات المعتمدة من الشركة الأم والمتاحة من داخل التطبيق
- 2 تعطيل خاصية مشاركة الشاشة لجميع المشاركين وعدم السماح بتصوير محتوى أو شاشات الاجتماعات المتعلقة بالعمل إلا بإذن من مضيف الاجتماع
- 3 إقتصار التواصل مع المدعويين للاجتماع فقط تجنباً لتمكين الغير من وضع برامج تجسس بالغرف الافتراضية للاجتماعات
- 4 إغلاق الانضمام للاجتماع بعد اكتمال عدد المشاركين والمدعويين وعدم السماح لغيرهم بالانضمام
- 5 استخدام أجهزة معتمدة من جهة العمل ومزودة ببرامج موصى باستخدامها
- 6 سرية وخصوصية الاجتماع من خلال التواجد في مكان آمن ومخصص للاجتماع
- 7 تعطيل خاصية الانضمام للاجتماع قبل حضور المضيف لمنع تسلل المتطفلين
- 8 مصدر رابط الاجتماع المُرسَل إذا كان هناك دعوة لحضور اجتماع عن بعد
- 9 مصادر رسائل البريد الإلكتروني المُستلمة
- 10 تسجيل الخروج الآمن من البرامج والتطبيقات المستخدمة في الاجتماع عن بعد والمغادرة فور الانتهاء من الاجتماع
- 11 استخدام خاصية "غرفة الانتظار" والتي تتيح للمشاركين الانتظار حتى يُسمح لهم بالانضمام للاجتماع
- 12 تعطيل خاصية السماح للمشاركين المستبعدة بالعودة للاجتماع مجدداً وذلك للحد من دخول المتصيدين
- 13 استخدام كلمة مرور قوية لغرف الاجتماعات ومشاركتها مع الغير بطريقة آمنة

من الأمور التي يجب تجنبها

عند استخدام التقنية في عقد الاجتماعات عن بعد:

