سياسة التخلص من صلاحيات الدخول

- يمكن أن يتسبب الدخول غير المصرح به إلى إلحاق ضرر خطير بعمادة تقنية المعلومات والإتصالات. ويمكن لموظفي العمادة استخدام طرق دخول ثابتة للدخول إلى الأنظمة أو المساحات الخاصة بالمكاتب. ويستطيع القراصنة استخدام حسابات غير نشطة للدخول على الأنظمة دون أن يلاحظهم أحد. وتشمل الأضرار المحتملة سرقة الأموال أو المعدات أو الملكية الفكرية أو الإفصاح عن المعلومات السرية و الأضرار المتعلقة بالممتلكات أو الأفراد.
- عندما يغادر شخص ما فإنه يجب إلغاء صلاحيات الدخول الخاصة به على الفور. ويتعين على الرئيس المشرف أن يبدأ في إزالة صلاحيات الدخول عن طريق قسم أمن المعلومات والأمن الصناعي. وعندما يغادر مجموعة من الموظفين، يتوجب على المشرف الخاص بهم ضمان أن يتم إلغاء صلاحيات الدخول الخاصة بهم سواء للأنظمة أو لمبنى العمادة. ويجب على الموظفين فقط امتلاك صلاحيات الدخول إلى مواقعهم. وعندما تتغير الأدوار، يجب على المشرفين أن يقوموا بسحب أية صلاحيات دخول غير ضرورية.
- هناك صلاحيات للدخول عن بعد إلى تطبيقات مخصصة وخوادم خاصة بالأنظمة. لذا يرجى إبلاغ قسم أمن المعلومات إذا لاحظت أن موظف سابق لديه القدرة على استخدام شبكة الجامعة.
- يبذل فريق أمن المعلومات جهوداً حثيثة لتعقب عمليات الدخول ونقضها.