

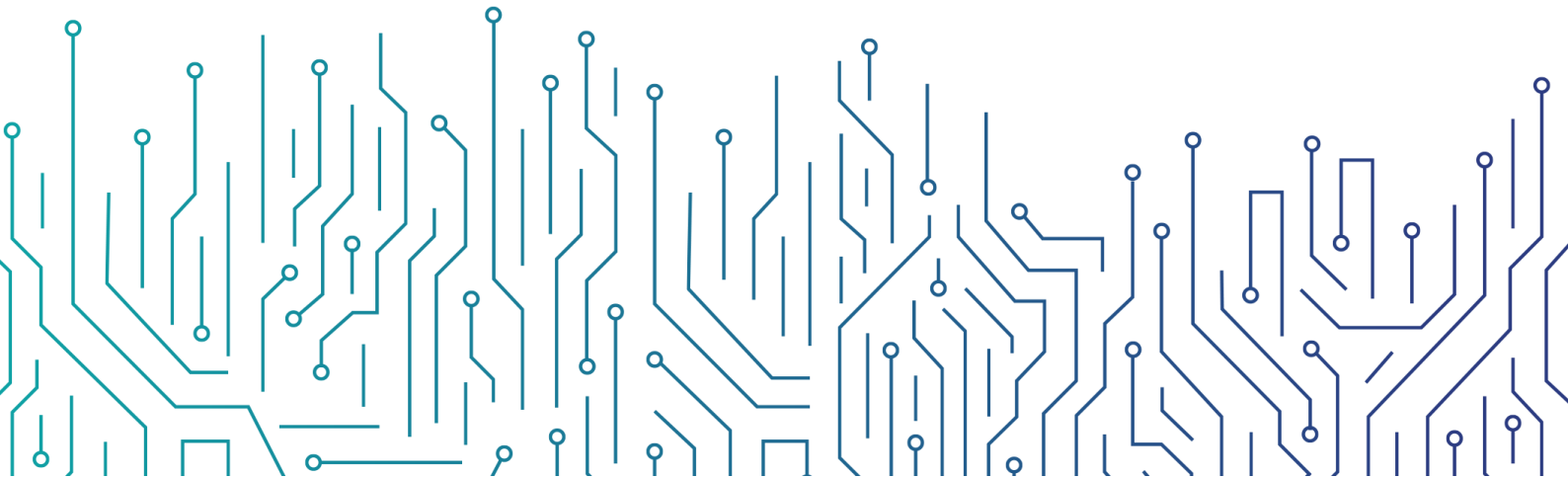


سياسة المكتب النظيف

التاريخ: 20/03/2025

الإصدار: 1.0

المرجع: الضوابط الأساسية للأمن السيبراني (ECC-٢: ٢٠٢٤)



● بنود السياسة

١- البنود العامة

- ١-١ يجب على منسوبي جامعة بيشة التأكد من تأمين جميع المعلومات الحساسة/السرية سواء كانت في شكل ورقي أو إلكتروني في أماكن عملهم في نهاية اليوم أو عند مغادرتهم لفترة طويلة..
- ٢-١ يجب تأمين أجهزة الكمبيوتر عند الخروج من المكتب وعند نهاية يوم العمل يجب.
- ٣-١ يجب إزالة أي معلومات مقيدة أو حساسة من سطح المكتب وتخزينها في درج مغلق عند عدم وجود الموظف بالمكتب وعند نهاية يوم العمل.
- ٤-١ يجب إبقاء الخزائن التي تحتوي على معلومات مقيدة أو حساسة مغلقة ومقفلة عندما لا تكون قيد الاستخدام أو عند عدم الإشراف عليها.
- ٥-١ يجب عدم ترك المفاتيح المستخدمة للوصول إلى المعلومات المقيدة أو الحساسة على مكتب غير مراقب.
- ٦-١ يجب أن تقيّد جامعة بيشة استخدام وسائط التخزين الخارجية وتوفر سبل التعامل الآمن معها.
- ٧-١ يجب تأمين أجهزة الكمبيوتر المحمولة إما باستخدام كابل قفل أو وضعها في درج مغلق عند عدم استخدامها وعند نهاية يوم العمل.
- ٨-١ يجب عدم ترك كلمات المرور مكتوبة على ملاحظات لاصقة ملصقة على الحاسوب أو تحته، كما لا يجوز كتابتها يجب إزالة المطبوعات التي تحتوي على معلومات مقيدة أو حساسة فوراً من الطابعة. في مكان يسهل الوصول إليه وفقاً لمعيار حماية كلمات المرور.
- ٩-١ عند التخلص من الوثائق المقيدة و/أو الحساسة، يجب تمزيقها في آلات التقطيع الرسمية أو وضعها في صناديق التخلص الآمنة المقفلة.
- ١٠-١ يجب مسح السبورات البيضاء التي تحتوي على معلومات مقيدة و/أو حساسة.
- ١١-١ يجب التعامل مع وسائط التخزين كما هو ملزم في ضوابط الأمن السيبراني بالتقييد الحازم لعدم استخدامها ويجب إزالة جميع المستندات من الطابعات وآلات الفاكس فور طباعتها

لضمان عدم ترك المستندات الحساسة في صناديق الطباعة حيث يمكن أن لغير المصرح لهم
بالوصول إليها.

انتهى،،