مخاطر الوثائق والمعلومات

مخاطر الوثائق والمعلومات:

هي مخاطر متوقعة بسبب أخطاء تقنية ومخاطر حفظ البيانات والمعلومات أو بسبب الأخطاء البشرية أو البيئية.

وتشمل ما يلي:

مخاطر تقنيّة:

1. خطر الاختراق.
2. خطر الفيروسات.
3. خطر.الدُّخول غير المُصرَّح به.
4. خطر استخدام النُّسخ غير الأصليّة من البرامج.
5. خطر التّعديل غير المُصرَّح به للبيانات أو المعلومات.
6. خطر دقّة البيانات والمعلومات وتوافقها وتكاملها.
7. خطر أعطال الأجهزة أو البرامج.

مخاطر بشرية:

8. خطر نقْص المهارات والكفاءات.
9. خطر الأخطاء البشريّة.
10. خطر سرقة الخوادم وأجهزة التخزين.

مخاطر بيئية ومخاطر بيئة العمل: :

11. خطر فقد البيانات بسبب الفيضانات، أو الحرائق، أو الزّلازل أو البراكين أو الحروب.
12. خطر التسرُّب المائيّ.
13. خطر انقطاع التكييف.
14. خطر انقطاع التيّار الكهربائيّ.
15. خطر انقطاع الدعم الفني والصيانة من مزودي الخدمات لمركز الحاسوب.

الجدول رقم (3) يبين مقياس تأثير مخاطر الوثائق والمعلومات عند حدوثها:

مخاطر الوثائق والمعلومات		
الرمز	**تأثير الخطر عند حدوثه**	**الآثار/ الأضرار**
E	منخفض جداً	حدث يحصل في مؤسسات أخرى وليس الجامعة
D	منخفض	حدث مرة واحدة في الجامعة
C	متوسط	حدث يحصل من وقت لآخر
B	خطير	حدث وقع عدة مرات أو أكثر عبر تاريخ الجامعة
A	شديد الخطورة	حدث متوقع حدوثه بشكل سنوي

مخاطر الوثائق والمعلومات: خطر الاختراق (Hacking)		
الخطر المتوقع	**بيانات الموقع**	**الشخص المسؤول**
مخاطر تقنيّة: الاختراق(Hacking)	جميع مرافق الجامعة التي تحوي أجهزة حاسوبية والخوادم الرئيسية في مركز الحاسوب المكان:جامعة الزيتونة الأردنية	الوظيفة: مدير مركز الحاسوب
وصف الخطر: الدخول الجَبريّ وكسر الحواجز والجُدُر الناريّة الواقية للخوادم والأجهزة التي تخدم البرامج والأنظمة.		
نوع الخطر: وثائق ومعلومات		
احتمالية حدوث الخطر: ☐ عالي جدا ☐ عالي ☐ متوسط ☑ منخفض ☐ منخفض جداً		
تأثير الخطر حال حدوثه: ☑ شديد الخطورة ☐ خطير ☐ متوسط ☐ منخفض ☐ منخفض جداً		

سياسة درء الخطر

1. عمل التّرتيبات الفنيّة المِهْنيّة اللّازمة من وضْع جُدُر ناريّة وتصميم الشّبكة بحيث تكون عَصيّة على الاختراق.
2. عمل اختبارات فنيّة منتظمة زمنيًّا لاختبار مدى التحصُّن.
3. تقصِّي التقنيات الجديدة والحديثة التي تمنع الاختراق.
4. متابعة الأداء الفنيّ لتقنيات منع الاختراق، وإصدار تقرير دوريٍ بذلك.

إجراء التعامل مع خطر الاختراق(Hacking)	
نوع الخطر:	الاختراق
مكان الخطر:	جميع مرافق الجامعة التي تحوي أجهزة حاسوبية والخوادم الرئيسية في مركز الحاسوب
الشخص المسؤول (للاتصال به عند وقوع الخطر):	مدير مركز الحاسوب
وسائل الاتصال به:	ايميل: compcenter@zuj.edu.jo هاتف 4291511 فرعي 200
الإجراء الفوري حال العلم بالخطر	فصل الجهاز المخترَق عن الشّبكة والاتّصال بالمسؤول مباشرة.
الجهة المسؤولة عن معالجة الخطر:	مركز الحاسوب.

الإجراءات المتخذة لمعالجة الخطر

1. تقليل تأثير الاختراق عن طريق عزْل الأنظمة المتضرّرة والتأكّد من حماية الأنظمة الأخرى.
2. تجهيز الفريق الأمنيّ المسؤول وتحديده حسْب نوع الاختراق(اختراق في أنظمة الشبكة، أو الأنظمة المساندة، أو اختراق بدنيّ).
3. البَدء بالبحث والتدقيق لتحديد أسباب الاختراق ومداه، وتحديد مقدار الضَّرر وإيجاد خطط بديلة.
4. البَدء بحلّ المشاكل وحماية النّظام من أيّ اختراق مماثل مستقبليّ.
5. رفع تقرير الى رئاسة الجامعة عن المشكلة ومدى ضررها وكيفيّة حلّها وتوعية المستخدِمين والموظَّفين.

انهاء الخطر والتخلص من الأضرار التي سببها:

1. إقفال الأنظمة المخترَقة أو عزلها حتى لا تتمكّن من الوصول إلى غيرها أو التأثير فيها.
2. استخدام أجهزة الجُدُر الناريّة وأجهزة الاختراق الشبكيّة لإيقاف الهجوم ومنع الوصول إلى الأنظمة.
3. عدم تشغيل الأنظمة المتضرّرة إلّا بعد اختبارها والتأكّد من خلُّوها من نقاط الضّعف.

مخاطر الوثائق والمعلومات: خطر الفيروسات		
الخطر المتوقع	**بيانات الموقع**	**الشخص المسؤول**
مخاطر تقنيّة: الفيروسات	جميع مرافق الجامعة التي تحوي أجهزة حاسوبية، الخوادم الرئيسية في مركز الحاسوب المكان:جامعة الزيتونة الأردنية	الوظيفة: مدير مركز الحاسوب
وصف الخطر: خطر تسرب الفيروسات: وهي برامج اذا ما اخترقت الخوادم ربما تسبب دمار أو فقد للبيانات او المعلومات او غيرها من الاضرار التي تسببها الفيروسات.		
نوع الخطر: وثائق ومعلومات		
احتمالية حدوث الخطر: ☐ عالي جدا ☐ عالي ☐ متوسط ☑ منخفض ☐ منخفض جداً		
تأثير الخطر حال حدوثه: ☐ شديد الخطورة ☑ خطير ☐ متوسط ☐ منخفض ☐ منخفض جداً		

سياسة درء الخطر

1. توافر إجراءات السّلامة والأمن الخاصّة بالمعلومات.
2. اتخاذ إجراءات، ووضْع سياسات لأمن المعلومات تخضع للمعايير العالميّة وأفضل الممارسات مثل(ISO 27000).
3. وضْع برامج مضادّات الفيروسات قيد التشغيل لمنع الفيروسات التي تهاجم الخوادم والأجهزة الرّئيسة في الجامعة والقضاء عليها.
4. التأكد من خلو الأجهزة غير المرتبطة بالخادم الرّئيسي من الفيروسات والتخلّص منها قبل الدّخول والارتباط بشبكة الجّامعة لتفادي الإصابة بالفيروسات.
5. تفعيل تحديث برنامج مضادّ الفيروسات بطريقة أوتوماتيكيّة لأيّ جهاز مرتبط بالشبكة الرئيسة للجامعة عن طريق الارتباط بال(Domain).

إجراء التعامل مع خطر الفيروسات	
نوع الخطر:	مخاطر تقنية: الفيروسات
مكان الخطر:	جميع مرافق الجامعة التي تحوي أجهزة حاسوبية، الخوادم الرئيسية في مركز الحاسوب
الشخص المسؤول (للاتصال به عند وقوع الخطر)	الوظيفة: مدير مركز الحاسوب
وسائل الاتصال به:	ايميل: compcenter@zuj.edu.jo هاتف 4291511 فرعي 200
الإجراء الفوري حال العلم بالخطر	فصل الجهاز المخترَق عن الشّبكة والاتّصال بالمسؤول مباشرة.
الجهة المسؤولة عن معالجة الخطر:	مركز الحاسوب / شعبة الشبكات والإتصالات

الإجراءات المتخذة لمعالجة الخطر

1. تقليل تأثير الفيروس بفصل النّظام أو عزله من قِبل المسؤول عن النّظام أو فريق شعبة الشبكات والإتصالات.
2. فحص النّظام من قِبل فريق شعبة الشبكات والإتصالات ، وتحديد الأضرار، وإمكانية إيجاد بدائل لاستمراريّة الخدمة أثناء حلّ المشكلة.
3. البَدء بتحليل الفيروس وإزالته، والاستعانة بالنُّسَخ الاحتياطيّة إن لزم الأمر وحماية النّظام كما يجب.
4. رفع تقرير الى رئاسة الجامعة عن المشكلة ومدى ضررها وكيفية حلّها، وتوعية المستخدِمِين والموظَّفِين.

انهاء الخطر والتخلص من الأضرار التي سببها:

1. استخدام برمجيات مكافحة الفيروسات ذات إدارة موحدة وأجهزة موانع الإختراق للشبكة .
2. التاكد من خلو الفيروس في الأجهزة المصابة .
3. عدم تشغيل الأنظمة المتضرّرَة إلّا بعد اختبارها والتأكّد من خلوّها من أيّ فيروس.
4. تحديث الأجهزة الواقية من الفيروسات بالنُّسخة الجديدة من عناوين الفيروسات.

مخاطر الوثائق والمعلومات: خطر الدُّخول غير المُصرَّح به (Unauthorized Access)		
الخطر المتوقع	**بيانات الموقع**	**الشخص المسؤول**
مخاطر تقنيّة: الدّخول غير المُصرَّح به (Unauthorized Access).	جميع مرافق الجامعة التي تحوي أجهزة حاسوبية، الخوادم الرئيسية في مركز الحاسوب المكان:جامعة الزيتونة الأردنية	الوظيفة: مدير مركز الحاسوب
وصف الخطر: الدّخول بطريقة غير مُصرّح بها إلى الأنظمة أو البرامج أو قواعد البيانات، وذلك عن طريق الحصول على اسم المستخدِم أو كلمة السِّر بطريقة غير مشروعة.		
نوع الخطر: وثائق ومعلومات		
احتمالية حدوث الخطر: ☐ عالي جدا ☐ عالي ☐ متوسط ☐ منخفض ☑ منخفض جداً		
تأثير الخطر حال حدوثه: ☐ شديد الخطورة ☑ خطير ☐ متوسط ☐ منخفض ☐ منخفض جداً		

سياسة درء الخطر

1. توافر إجراءات السّلامة والأمن الخاصّة بالمعلومات.
2. وضع إجراءات وسياسات لأمن المعلومات تخضع للمعايير العالميّة، وأفضل الممارسات مثل(ISO 27000) التي تضع إجراءات الدّخول وسياساته.
3. تعزيز التوعية بأمن المعلومات، وحفظ كلمات السّر، وطرائق تحصينها.
4. عمل اختبارات دوريّة لفحص إمكانية الدّخول غير المُصرَّح به.

إجراء التعامل مع خطر الدخول غير المصرح به Unauthorized Access	
نوع الخطر:	الدخول غير المصرح به Unauthorized Access
مكان الخطر:	جميع مرافق الجامعة التي تحوي أجهزة حاسوبية، الخوادم الرئيسية في مركز الحاسوب
الشخص المسؤول (للاتصال به عند وقوع الخطر):	مدير مركز الحاسوب.
وسائل الاتصال به:	ايميل: compcenter@zuj.edu.jo هاتف 4291511 فرعي 200
الإجراء الفوري حال العلم بالخطر:	الاتّصال بالمسؤول مباشرة.
الجهة المسؤولة عن معالجة الخطر:	مدير مركز الحاسوب / شعبة الشبكات والإتصالات

الإجراءات المتخذة لمعالجة الخطر

1. تقليل تأثير الخطر بإيقاف الحساب المستخدَم للدّخول أو بعزْل النّظام المتضرّر والتأكّد من حماية الأنظمة الأخرى.
2. ارسال الفريق التقنيّ المسؤول عن الأنظمة المتضرّرة وتحديده.
3. البَدء بالبحث والتدقيق لتحديد كيفيّة الدّخول والتغيُّرات التي حصلت لتحديد الضَّرر.
4. حماية النّظام، ومنع تكرار المشكلة، واسترجاع ما غُيِّر أو إزالة ما أُضيف.
5. رفع تقرير الى رئاسة الجامعة عن المشكلة وكيفيّة حلّها، ومدى الضَّرر الحاصل، وتوعية المستخدِمين والموظَّفين.

انهاء الخطر والتخلص من الأضرار التي سببها:

1. إيقاف الحساب المستخدَم مؤقتا أو تغيير كلمة السِّر.
2. عزْل الأنظمة المتضرّرَة إن وُجِدت.

مخاطر الوثائق والمعلومات: خطر استخدام النُّسخ غير الأصليّة من البرامج		
الخطر المتوقع	**بيانات الموقع**	**الشخص المسؤول**
مخاطر تقنيّة: استخدام النُّسخ غير الأصليّة من البرامج.	جميع مرافق الجامعة التي تحوي أجهزة حاسوبية، الخوادم الرئيسية في مركز الحاسوب المكان:جامعة الزيتونة الأردنية	الوظيفة: مدير مركز الحاسوب
وصف الخطر: استخدام نسخ غير مرخصة من البرامج أو الأنظمة التي تخدم العمل، ما قد يُسبِّب التوقُّف في لحظة ما خلال العمل، أو عدم المقدرة على إجراء أعمال على تلك البرامج، بسبب توقُّفها لأنّها غير مُرخَّصة.		
نوع الخطر: وثائق ومعلومات		
احتمالية حدوث الخطر: ☐ عالي جدا ☐ عالي ☐ متوسط ☑ منخفض ☐ منخفض جداً		
تأثير الخطر حال حدوثه: ☐ شديد الخطورة ☑ خطير ☐ متوسط ☐ منخفض ☐ منخفض جداً		

سياسة درء الخطر:

1. حصْر البرامج والأنظمة التي تحتاج إلى رُخَص بطريقة دوريّة.
2. توافر الرُّخَص.
3. إنشاء بريد إلكتروني خاص للإبلاغ عن البرامج التي تُستَخدَم بطريقة غير مشروعة.

إجراء التعامل مع خطر استخدام النُّسخ غير الأصليّة من البرامج	
نوع الخطر:	استخدام النُسَخ غير الأصليّة من البرامج.
مكان الخطر:	جميع مرافق الجامعة التي تحوي أجهزة حاسوبية، الخوادم الرئيسية في مركز الحاسوب
الشخص المسؤول (للاتصال به عند وقوع الخطر)	الوظيفة: مدير مركز الحاسوب
وسائل الاتصال به:	ايميل: compcenter@zuj.edu.jo هاتف 4291511 فرعي 200
الإجراء الفوري حال العلم بالخطر	ابلاغ المسؤول مباشرة
الجهة المسؤولة عن معالجة الخطر:	مدير مركز الحاسوب / شعبة الحواسيب وملحقاتها

الإجراءات المتخذة لمعالجة الخطر

1. إيقاف استخدام أيّ جهاز يستخدم برامج غير مُرخَّصة.
2. توفير واستخدام برامج مرُخَّصة بدلًا من غير المرخَّصة.

انهاء الخطر والتخلص من الأضرار التي سببها:

1. توعية العاملين بسياسات عدم استخدام النسخ غير الاصلية وذلك حفاظا على حقوق الملكية الفكرية.
2. اتخاذ الإجراءات المناسبة بحق الاشخاص المخالفين لاستخدام النسخ غير الاصلية.

مخاطر الوثائق والمعلومات: خطر التّعديل غير المُصرَّح به للبيانات أو المعلومات		
الخطر المتوقع	**بيانات الموقع**	**الشخص المسؤول**
مخاطر تقنيّة: خطر التّعديل غير المُصرَّح به للبيانات أو المعلومات.	جميع مرافق الجامعة التي تحوي أجهزة حاسوبية والخوادم الرئيسية في مركز الحاسوب المكان:جامعة الزيتونة الأردنية	الوظيفة: مدير مركز الحاسوب
وصف الخطر: الدّخول بطريقة غير مُصرَّح بها إلى الأنظمة أو البرامج أو قواعد البيانات، وذلك عن طريق الحصول على اسم المستخدِم أو كلمة السِّر بطريقة غير مشروعة، ومن ثَمّ تعديل البيانات، وربّما يكون ذلك التّعديل عن طريق استغلال موقع مُحدَّد لتعديل البيانات والمعلومات بغير وجْه حق.		
نوع الخطر: وثائق ومعلومات		
احتمالية حدوث الخطر: ☐ عالي جدا ☐ عالي ☐ متوسط ☐ منخفض ☑ منخفض جداً		
تأثير الخطر حال حدوثه: ☐ شديد الخطورة ☑ خطير ☐ متوسط ☐ منخفض ☐ منخفض جداً		

سياسة درء الخطر:

1. وضع إجراءات وسياسات لأمن المعلومات تخضع للمعايير العالميّة، وأفضل الممارسات مثل (ISO 27000) التي تحدد إجراءات الدخول وسياساته.
2. تعزيز التوعية بأمن المعلومات، وحفظ كلمات السِّر، وطرائق تحصينها وعمل اختبارات دوريّة لفحص إمكانيّة التّعديل غير المُصرَّح به للبيانات أو المعلومات.
3. عمل تقرير دوريّ لحصر التّعديل غير المُصرَّح به للبيانات أو المعلومات إنْ وُجِد.

.

إجراء التعامل مع خطر التّعديل غير المُصرَّح به للبيانات أو المعلومات	
نوع الخطر:	التّعديل غير المُصرَّح به للبيانات أو المعلومات.
مكان الخطر:	جميع انظمة تقنية المعلومات والاتصالات والخدمات الالكترونية
الشخص المسؤول (للاتصال به عند وقوع الخطر)	مدير مركز الحاسوب
وسائل الاتصال به:	ايميل: compcenter@zuj.edu.jo هاتف 4291511 فرعي 200
الإجراء الفوري حال العلم بالخطر	الاتّصال بالمسؤول مباشرة.
الجهة المسؤولة عن معالجة الخطر:	مدير مركز الحاسوب / شعبة الشبكات والإتصالات / شعبة البرمجة والويب.

الإجراءات المتخذة لمعالجة الخطر

1. تقليل تأثير الخطر بعزْل الأنظمة المتضرِّرَة إن أمكن أو إيقاف الحساب المستخدَم أو المشكوك فيه والتأكّد من حماية الأنظمة الأخرى.
2. تجهيز الفريق التقنيّ المسؤول عن الأنظمة المتضرِّرَة وتحديده.
3. البَدء بالبحث والتدقيق لتحديد كيفيّة الدّخول والتغييرات التي حصلت وتأثيرها لتحديد الضَّرر.
4. حلّ المشكلة، وحماية النّظام لمنع تكرار الضَّرر، والعودة إلى نقطة التشغيل الصحيحة.
5. رفع تقرير الى رئاسة الجامعة عن المشكلة ومدى الضَّرر الحاصل وكيفيّة حلّها وتوعية المستخدِمين والموظَّفِين.

انهاء الخطر والتخلص من الأضرار التي سببها:

1. إعادة البيانات إلى ما كانت عليه قبل التّعديل غير المصرَّح به عن طريق نُسَخ الأمان.
2. تغيير كلمة الدّخول أو كلمة السِّر للمستخدِم المسيء أو إلغاؤها.

مخاطر الوثائق والمعلومات: خطر دقة البيانات والمعلومات وتوافقها وتكاملها		
الخطر المتوقع	**بيانات الموقع**	**الشخص المسؤول**
مخاطر تقنيّة: دقّة البيانات والمعلومات وتوافقها وتكامله.ا	جميع مرافق الجامعة التي تحوي أجهزة حاسوبية، الخوادم الرئيسية في مركز الحاسوب المكان:جامعة الزيتونة الأردنية	مدير مركز الحاسوب
وصف الخطر: يتمثّل هذا الخطر في إدخال بيانات غير دقيقة أو خاطئة أو وجودها مما يسبّب مخرجات غير دقيقة وخاطئة، كذلك عدم توافق البيانات المُدخَلَة وعدم تكاملها.		
نوع الخطر: وثائق ومعلومات		
احتمالية حدوث الخطر: ☐ عالي جدا ☐ عالي ☐ متوسط ☐ منخفض ☑ منخفض جداً		
تأثير الخطر حال حدوثه: ☐ شديد الخطورة ☐ خطير ☑ متوسط ☐ منخفض ☐ منخفض جداً		

سياسة درء الخطر:

1. استخدام منهجيّات تطوير الأنظمة المعمول بها عالميًّا وطبقًا لأفضل الممارسات والمنهجيّات الفنيّة بذلك.
2. عمل اختبارات دوريّة لفحص دقّة البيانات وتطابقها.
3. تخصيص خطوط تواصل خاصّة بخدمة المستخدمين ، للإبلاغ عن أيّ تناقض أو عدم دقّة في البيانات والمعلومات وتطابقها مع بعضها بعضًا.

.

إجراء التعامل مع خطر دقة البيانات والمعلومات وتوافقها وتكاملها	
نوع الخطر:	مخاطر تقنيّة: دقّة البيانات والمعلومات وتوافقها.
مكان الخطر:	جميع الانظمة والخدمات الالكترونية
الشخص المسؤول (للاتصال به عند وقوع الخطر)	مدير مركز الحاسوب.
وسائل الاتصال به:	ايميل: compcenter@zuj.edu.jo هاتف 4291511 فرعي 200
الإجراء الفوري حال العلم بالخطر	الاتّصال بالمسؤول مباشرة.
الجهة المسؤولة عن معالجة الخطر:	مدير مركز الحاسوب.

الإجراءات المتخذة لمعالجة الخطر

1. تقليل تأثير الخطر بعزْل الأنظمة المتضرّرة إن أمكن أو إيقاف الحساب المستخدَم أو المشكوك فيه، والتأكّد من حماية الأنظمة الأخرى.
2. تحديد الفريق التقنيّ المسؤول عن الأنظمة المتضرّرة وتجهيزه.
3. البَدء بالبحث والتدقيق لتحديد مكامن عدم دقّة البيانات وتوافقها.
4. حلّ المشكلة لمنع تكرار الضَّرر، والعودة إلى البيانات الصحيحة.
5. إرسال تقرير عن المشكلة وكيفية حلّها، ومدى الضرر الحاصل، وتوعية المستخدِمين والموظَّفين.

انهاء الخطر والتخلص من الأضرار التي سببها:

إعادة البيانات إلى ما كانت عليه قبل اكتشاف عدم دقة البيانات أو توافقها عن طريق نُسَخ الأمان.

مخاطر الوثائق والمعلومات: خطر أعطال الأجهزة أو البرامج		
الخطر المتوقع	**بيانات الموقع**	**الشخص المسؤول**
مخاطر تقنيّة: أعطال الأجهزة أو البرامج	جميع مرافق الجامعة التي تحوي أجهزة حاسوبية، الخوادم الرئيسية في مركز الحاسوب المكان: جامعة الزيتونة الأردنية	الوظيفة: مدير مركز الحاسوب.
وصف الخطر: يتمثّل هذا الخطر في تعطُّل الأجهزة الرئيسة للجامعة، أو البرامج والأنظمة التي تخدم أهمّ العمليّات أو الخدمات التي تقدّمها الجامعة، وهذا الخطر يتمثّل في انقطاع الخدمات عن المستفيدِين في الجامعة.		
نوع الخطر: وثائق ومعلومات		
احتمالية حدوث الخطر: ☐ عالي جدا ☐ عالي ☐ متوسط ☑ منخفض ☐ منخفض جداً		
تأثير الخطر حال حدوثه: ☐ شديد الخطورة ☐ خطير ☑ متوسط ☐ منخفض ☐ منخفض جداً		

سياسة درء الخطر:

1. التفتيش الدوري على الاجهزة والبرامج.
2. إجراء عمليّات الصيانة الدوريّة للأجهزة والبرامج.
3. عمل عقود صيانة سريعة الخدمة في حال التوقّف.
4. تخصيص فِرَق عمل جاهزة للطوارئ خاصّة بالأجهزة أو البرامج..

إجراء التعامل مع خطر أعطال الأجهزة أو البرامج	
نوع الخطر:	أعطال الأجهزة أو البرامج
مكان الخطر:	جميع مرافق الجامعة التي تحوي أجهزة حاسوبية والخوادم الرئيسية في مركز الحاسوب
الشخص المسؤول (للاتصال به عند وقوع الخطر)	مدير مركز الحاسوب
وسائل الاتصال به:	ايميل: compcenter@zuj.edu.jo هاتف 4291511 فرعي 200
الإجراء الفوري حال العلم بالخطر	الاتّصال بالمسؤول مباشرة
الجهة المسؤولة عن معالجة الخطر:	مركز الحاسوب / شعبة الحواسيب وملحقاتها

الإجراءات المتخذة لمعالجة الخطر

1. تجهيز الفريق التقنيّ المسؤول عن الأنظمة المتعطِّلة أو الأجهزة.
2. البَدء بالبحث والتدقيق لتحديد مشكلة التعطُّل والعمل على حصرها .
3. حلّ المشكلة ومنع تكرار التعطُّل والعودة إلى البيانات الصحيحة.
4. رفع تقرير الى رئاسة الجامعة عن المشكلة وكيفية حلّها، ومدى الضَّرر الحاصل، وتوعية المستخدِمين والموظَّفِين.

انهاء الخطر والتخلص من الأضرار التي سببها:

إعادة البيانات إلى ما كانت عليه قبل التعطُّل عن طريق نُسخ الأمان إذا كانت هناك أضرار في البيانات.

مخاطر الوثائق والمعلومات:خطر فَقْد البيانات بسبب الفيضانات أو الحرائق أو الزّلازل والبراكين أو الحروب		
الخطر المتوقع	**بيانات الموقع**	**الشخص المسؤول**
مخاطر طبيعيّة: فقْد البيانات بسبب الفيضانات، أو الحرائق أو الزلازل أو البراكين، أو الحروب.	جميع مرافق الجامعة التي تحوي أجهزة حاسوبية والخوادم الرئيسية في مركز الحاسوب المكان: جامعة الزيتونة الأردنية	الوظيفة: مدير مركز الحاسوب
وصف الخطر: فقْد البيانات والمعلومات بسبب الفيضانات أو الحرائق أو الزلازل أو البراكين أو الحروب عن طريق إغراق أو حرق أو تدمير مركز المعلومات والأجهزة الخادمة الموجودة فيه التي تحتوي البيانات والمعلومات الموجودة في الجامعة.		
نوع الخطر: وثائق ومعلومات		
احتمالية حدوث الخطر: ☐ عالي جدا ☐ عالي ☐ متوسط ☐ منخفض ☑ منخفض جداً		
تأثير الخطر حال حدوثه: ☐ شديد الخطورة ☐ خطير ☑ متوسط ☐ منخفض ☐ منخفض جداً		

سياسة درء الخطر:

1. تطوير خُطّة تخطِّي الكوارث تختصُّ بإجراءات تخطِّي الكوارث ومنها الفيضانات.
2. عمل نسخة متكاملة من البيانات والمعلومات يوميًّا ووضعها في مكان آمن خارج محيط الجامعة والمنطقة وحسب المواصفات الفنيّة العالميّة.
3. توافر خزائن وأبواب مضادّة للحريق والماء لتحمي مركز المعلومات والأجهزة والخوادم.
4. إيجاد مركز معلومات بديل يحتوي الأجهزة والبرامج والأنظمة اللازمة لتشغيل أعمال تقنية المعلومات في الجامعة في حال تعطُّل مركز المعلومات الرئيس.

إجراء التعامل مع خطر فَقْد البيانات بسبب الفيضانات، أو الحرائق أو الزّلازل والبراكين أو الحروب	
نوع الخطر:	فقْد البيانات بسبب الفيضانات، أو الحرائق أو الزلازل أو البراكين، أو الحروب
مكان الخطر:	مراكز البيانات المختلفه
الشخص المسؤول (للاتصال به عند وقوع الخطر)	مدير مركز الحاسوب
وسائل الاتصال به:	ايميل: compcenter@zuj.edu.jo هاتف 4291511 فرعي 200
الإجراء الفوري حال العلم بالخطر	ابلاغ رئيس الجامعة
الجهة المسؤولة عن معالجة الخطر:	مركز الحاسوب.

الإجراءات المتخذة لمعالجة الخطر

1. التّنسيق مع دائرة الهندسة والصيانة والخدمات للتأكّد من عدم وجود أيّ خطر كهربائيّ في موقع الكارثة.
2. فصل التيار الكهربائي عن غرفة الخوادم.
3. تحديد الفريق الشبكيّ والأمنيّ وتجهيزه لمعاينة الموقع وتحديد مدى الضّرَر وما يحتاج إليه الفريق لإعادة الخدمة.
4. إيجاد حلول بديلة للمستخدِمين المتضرّرين بتوصيلهم إلى أجهزة شبكيّة مؤقّتة ومركز البيانات البديل.
5. بعد تأكُّد دائرة الهندسة والصيانة والخدمات من تجهيز اللازم من تكييف وكهرباء، تُجهَّز الأجهزة الشبكيّة والنُسَخ الاحتياطيّة.
6. إرسال تقرير عن تفصيلات المهمّة لإعلام الإدارة التنفيذيّة والمختَصّين بالمهمّة.
7. التّنسيق مع دائرة الهندسة والصيانة والخدمات للتأكُّد من عدم وجود أيّ خطر في الموقع وللسَّماح بالدّخول.
8. تحديد تجهيز الفريق التقنيّ وتجهيزه لمعاينة الموقع، وتحديد مستوى الضَّرّر وما قد يحتاج إليه لإعادة الخدمة.
9. إيجاد حلول بديلة للمستخدِمين المتضرّرين بتوصيلهم إلى أنظمة مؤقَّتة ومركز البيانات البديل.
10. بعد التأكُّد من الانتهاء من الغُرَف الشبكيّة(تكييف وكهرباء....) تُجهَّز الأجهزة وتُفَعَّل.
11. ارسال تقرير عن تفصيلات المهمّة لإعلام الإدارة التنفيذيّة والمختصّين.

انهاء الخطر والتخلص من الأضرار التي سببها:

إعادة البيانات عن طريق نسخ الأمان ومركز البيانات البديل.

مخاطر الوثائق والمعلومات: خطر سرقة الخوادم وأجهزة التخزين		
الخطر المتوقع	**بيانات الموقع**	**الشخص المسؤول**
مخاطر بشريّة: سرقة الخوادم ، مواد وأجهزة التخزين.	مركز الحاسوب المكان:جامعة الزيتونة الأردنية	الوظيفة: مدير مركز الحاسوب
وصف الخطر: فقْد البيانات والمعلومات في حال سرقة الخوادم من مراكز البيانات.		
نوع الخطر: وثائق ومعلومات		
احتمالية حدوث الخطر: ☐ عالي جدا ☐ عالي ☐ متوسط ☐ منخفض ☑ منخفض جداً		
تأثير الخطر حال حدوثه: ☑ شديد الخطورة ☐ خطير ☐ متوسط ☐ منخفض ☐ منخفض جداً		

سياسة درء الخطر:

1. التأكد من إجراءات السّلامة والأمن الخاصّة بالمعلومات.
2. التاكد من عمل كاميرات المراقبة لمراكز البيانات.
3. توافر إجراءات وسياسات صارمة للدّخول إلى مراكز البيانات.

إجراء التعامل مع خطر سرقة الخوادم وأجهزة التخزين	
نوع الخطر:	سرقة الخوادم وأجهزة التخزين.
مكان الخطر:	مركز الحاسوب
الشخص المسؤول (للاتصال به عند وقوع الخطر)	مدير مركز الحاسوب
وسائل الاتصال به:	ايميل: compcenter@zuj.edu.jo هاتف 4291511 فرعي 200
الإجراء الفوري حال العلم بالخطر	ابلاغ رئيس الجامعة
الجهة المسؤولة عن معالجة الخطر:	مركز الحاسوب.

الإجراءات المتخذة لمعالجة الخطر:

1. التّحقُّق من الفاعل عن طريق الكاميرات الموجودة، والسجلّات الخاصّة بالدّخول والخروج.
2. إيقاف جميع الأنظمة والأجهزة المرتبطة بالجهاز المسروق.
3. إلغاء الجهاز المسروق من دائرة الارتباط مع الأنظمة والأجهزة الأخرى.
4. العمل على توفير بديل عن الجهاز المسروق.
5. إعادة العمل إلى ما كان عليه.
6. إيجاد الفاعل، وتقديم الوثائق إلى الدّائرة القانونيّة.
7. إرسال تقرير عن تفصيلات المهمّة لإعلام الإدارة التنفيذيّة والمختصِّين.

انهاء الخطر والتخلص من الأضرار التي سببها:

إلغاء وظائف الجهاز المسروق من دائرة الارتباط مع الأنظمة والأجهزة الأخرى، وإعادة البيانات إلى ما كانت عليه في حالة تعديل بيانات.

مخاطر الوثائق والمعلومات: خطر نقص المهارات والكفاءات		
الخطر المتوقع	**بيانات الموقع**	**الشخص المسؤول**
مخاطر بشريّة: نقص المهارات والكفاءات.	مركز الحاسوب المكان:جامعة الزيتونة الأردنية	الوظيفة: مدير مركز الحاسوب
وصف الخطر: يتمثّل هذا الخطر في عدم توافر الكفاءات والمهارات الخاصة بتقنية المعلومات والاتصالات أو نقْصها أو تسرُّبها.		
نوع الخطر: وثائق ومعلومات		
احتمالية حدوث الخطر: ☐ عالي جدا ☐ عالي ☑ متوسط ☐ منخفض ☐ منخفض جداً		
تأثير الخطر حال حدوثه: ☐ شديد الخطورة ☐ خطير ☑ متوسط ☐ منخفض ☐ منخفض جداً		

سياسة درء الخطر:

1. توافر خطط تدريبيّة للاحتياجات الوظيفيّة لتقنية المعلومات والاتّصالات.
2. عمل خطط لتحفيز الموظَّفِين بهدف استبقائهم واستقطاب ذوي الخبرات الخارجيّة.
3. تطبيق برامج تدريبيّة لموظَّفِي تقنية المعلومات والاتّصالات تساعد على رفع الكفاءات والمهارات.
4. مراقبة نسبة الاستبقاء والاستقطاب والتسرُّب ومتابعتها بصورة دوريّة لموظَّفِي تقنية المعلومات والاتّصالات.
5. توافر بدائل التّوظيف الخارجيّ للكفاءات والمهارات المتميّزة.

إجراء التعامل مع خطر نقص المهارات والكفاءات	
نوع الخطر:	نقص المهارات والكفاءات
مكان الخطر:	مركز الحاسوب
الشخص المسؤول (للاتصال به عند وقوع الخطر)	مدير مركز الحاسوب
وسائل الاتصال به:	ايميل: compcenter@zuj.edu.jo هاتف 4291511 فرعي 200
الإجراء الفوري حال العلم بالخطر	ابلاغ رئيس الجامعة
الجهة المسؤولة عن معالجة الخطر:	مركز الحاسوب.

الإجراءات المتخذة لمعالجة الخطر:

1. الإيعاز إلى الموظف البديل في المهارة المعيّنة لتعويض النَّقص.
2. تدريب أفراد آخرين على الكفاءات والمهارات المطلوبة.
3. تحديث خُطّة التّدريب والاستقطاب لإيجاد بدائل جديدة.
4. التنسيق مع دائرة شؤون العاملين لتعيين أصحاب كفاءات جديدة.

انهاء الخطر والتخلص من الأضرار التي سببها:

التعاقد مع جهات خارجية.

مخاطر الوثائق والمعلومات: خطر الأخطاء البشرية (Human Errors)		
الخطر المتوقع	**بيانات الموقع**	**الشخص المسؤول**
مخاطر بشريّة: أخطاء بشريّة (Human Errors)	جميع مرافق الجامعة التي تحوي أجهزة حاسوبية والخوادم في مركز الحاسوب المكان:جامعة الزيتونة الأردنية	الوظيفة: مدير مركز الحاسوب .
وصف الخطر: يتمثّل هذا الخطر في حدوث أخطاء بشريّة غير متعمّدة أثناء تأدية أعمال تقنية المعلومات والاتّصالات ما يؤثر في أداء الأجهزة أو الأنظمة أو أجهزة الاتّصالات الشبكيّة		
نوع الخطر: وثائق ومعلومات		
احتمالية حدوث الخطر: ☐ عالي جدا ☐ عالي ☐ متوسط ☑ منخفض ☐ منخفض جداً		
تأثير الخطر حال حدوثه: ☐ شديد الخطورة ☐ خطير ☐ متوسط ☑ منخفض ☐ منخفض جداً		

سياسة درء الخطر:

1. توثيق أيّة متطلبات للتعديل حسب التعليمات النافذة ومن ثَمّ توثيق التعديلات التي أُجريت.
2. استخدام منهجيّة (ITIL) في إدارة التغيير.
3. عمل نُسَخ الأمان قبل وبعد إجراء التّعديلات.

إجراء التعامل مع خطر الأخطاء البشرية (Human Errors)	
نوع الخطر:	أخطاء بشريّة (Human Errors)
مكان الخطر:	مركز الحاسوب
الشخص المسؤول (للاتصال به عند وقوع الخطر)	مدير مركز الحاسوب
وسائل الاتصال به:	ايميل: compcenter@zuj.edu.jo هاتف 4291511 فرعي 200
الإجراء الفوري حال العلم بالخطر	الاتّصال بالمسؤول مباشرة.
الجهة المسؤولة عن معالجة الخطر:	مركز الحاسوب .

الإجراءات المتخذة لمعالجة الخطر:

1. إيقاف الجهاز أو النّظام الذي وقع فيه الخطأ البشريّ.
2. عزْل الجهاز أوالنّظام عن الشّبكة الرئيسة.
3. تحليل المشكلة والأخطاء وإيجاد الحلول.
4. توثيق ما حصل من خطأ وخلل على الجهاز أو النّظام.
5. إعادة الحالة إلى ما كانت عليه قبل وقوع الخطأ.
6. عمل تقرير عن ما حصل، وكيفية الحلّ ورفعه إلى رئاسة الجامعة.

انهاء الخطر والتخلص من الأضرار التي سببها:

إعادة البيانات إلى حالة ما قبل وقوع الخطأ عن طريق نُسَخِ الأمان.

مخاطر الوثائق والمعلومات: خطر انقطاع التيار الكهربائي		
الخطر المتوقع	**بيانات الموقع**	**الشخص المسؤول**
مخاطر بيئة العمل: انقطاع التيار الكهربائي.	جميع مرافق الجامعة التي تحوي أجهزة حاسوبية، والخوادم في مركز الحاسوب المكان:جامعة الزيتونة الأردنية	الوظيفة: مدير مركز الحاسوب، مدير دائرة الهندسة والصيانة والخدمات.
وصف الخطر: يتمثّل هذا الخطر في انقطاع الكهرباء عن مركز البيانات ومن ثَمّ تعطُّل الأجهزة المختلفة التي تقدّم خدمات تقنية المعلومات والاتّصالات للمستفيدِين.		
نوع الخطر: وثائق ومعلومات		
احتمالية حدوث الخطر: ☐ عالي جدا ☐ عالي ☑ متوسط ☐ منخفض ☐ منخفض جداً		
تأثير الخطر حال حدوثه: ☐ شديد الخطورة ☐ خطير ☐ متوسط ☑ منخفض ☐ منخفض جداً		

سياسة درء الخطر:

1. عمل صيانة دوريّة لمصادر الطاقة الكهربائية في مراكز البيانات.
2. توافر مصادر بديلة للطّاقة الكهربائيّة(مولدات) تعمل أوتوماتيكياً في حال توقُّف المصدر الرّئيس للكهرباء.
3. توافر فِرَق عمل خاصّة بالكهرباء تراقب الأعطال الكهربائيّة وتعمل على اصلاحها حال حدوثها.

إجراء التعامل مع خطر انقطاع التيار الكهربائي	
نوع الخطر:	انقطاع الكهرباء.
مكان الخطر:	مدير مركز الحاسوب
الشخص المسؤول (للاتصال به عند وقوع الخطر)	مدير مركز الحاسوب، مدير دائرة الهندسة الصيانة والخدمات
وسائل الاتصال به:	ايميل: compcenter@zuj.edu.jo هاتف 4291511 فرعي 200
الإجراء الفوري حال العلم بالخطر	الاتّصال بالمسؤول مباشرة
الجهة المسؤولة عن معالجة الخطر:	مركز الحاسوب، دائرة الهندسة والصيانة والخدمات

الإجراءات المتخذة لمعالجة الخطر:

1. تشغيل مصادر الطاقة الكهربائية البديلة .
2. البَدء بالبحث والتدقيق لتحديد مشكلة التعطُّل في الكهرباء.
3. حلّ المشكلة ومنع تكرار التعطُّل.
4. رفع تقرير الى رئاسة الجامعة عن المشكلة وكيفية حلّها، ومدى الضَّرر الحاصل، وتوعية المستخدِمِين والموظَّفِين.

انهاء الخطر والتخلص من الأضرار التي سببها:

إعادة البيانات إلى ما كانت عليه قبل التعطُّل عن طريق نُسَخ الأمان إذا كانت هناك أضرار في البيانات.

مخاطر الوثائق والمعلومات: خطر انقطاع التكييف		
الخطر المتوقع	**بيانات الموقع**	**الشخص المسؤول**
مخاطر بيئة العمل: انقطاع التكييف.	غرفة الخوادم في مركز الحاسوب المكان:جامعة الزيتونة الأردنية	الوظيفة: مدير مركز الحاسوب، مدير دائرة الهندسة والصيانة والخدمات
وصف الخطر: يتمثّل هذا الخطر في انقطاع التكييف عن مركز البيانات ومن ثَمّ تعطُّل الأجهزة المختلفة التي تقدم خدمات تقنية المعلومات والاتّصالات للمستفيدِين بسبب الحرارة المنبعثة منها.		
نوع الخطر: وثائق ومعلومات		
احتمالية حدوث الخطر: ☐ عالي جدا ☐ عالي ☑ متوسط ☐ منخفض ☑ منخفض جداً		
تأثير الخطر حال حدوثه: ☐ شديد الخطورة ☐ خطير ☑ متوسط ☐ منخفض ☐ منخفض جداً		

سياسة درء الخطر:

1. عمل صيانة دوريّة لأجهزة التكييف في مراكز البيانات.
2. التأكد من عمل بدائل للتكييف التي تعمل أوتوماتيكيا في حال توقُّف المصدر الرّئيس للتكييف.
3. توافر فِرَق عمل خاصّة بالتكييف تُراقب الأعطال وتصلحها حال حدوثها.
4. توافر مركز بيانات بديل ومؤقّت.

إجراء التعامل مع خطر انقطاع التكييف	
نوع الخطر:	انقطاع التكييف
مكان الخطر:	غرفة الخوادم الرئيسية في مركز الحاسوب
الشخص المسؤول (للاتصال به عند وقوع الخطر)	مدير مركز الحاسوب، مدير دائرة الهندسة والصيانة والخدمات
وسائل الاتصال به:	ايميل: compcenter@zuj.edu.jo maint@zuj.edu.jo هاتف 4291511 فرعي 200
الإجراء الفوري حال العلم بالخطر	الاتّصال بالمسؤول مباشرة
الجهة المسؤولة عن معالجة الخطر:	مركز الحاسوب، دائرة الهندسة والصيانة والخدمات

الإجراءات المتخذة لمعالجة الخطر:

1. تشغيل انظمة التكييف البديلة إن وُجِد أو إطفاء الأجهزة في حالة عدم وجود بديل.
2. البَدء بالبحث والتدقيق لتحديد مشكلة التعطُّل في التكييف.
3. حلّ المشكلة ومنع تكرار التعطُّل.
4. تشغيل الأجهزة وإعادة الوضع إلى ما كان عليه.
5. رفع تقرير الى رئاسة الجامعة عن المشكلة وكيفية حلّها، ومدى الضَّرَر الحاصل وتوعية المستخدِمين والموظَّفِين.

انهاء الخطر والتخلص من الأضرار التي سببها:

إعادة البيانات إلى ما كانت عليه قبل التعطُّل عن طريق نُسَخ الأمان إذا كانت هناك أضرار في البيانات.

مخاطر الوثائق والمعلومات: خطر التسرب المائي		
الخطر المتوقع	**بيانات الموقع**	**الشخص المسؤول**
مخاطر بيئة: التسرُّب المائيّ.	مركز الحاسوب المكان:جامعة الزيتونة الأردنية	الوظيفة: مدير مركز الحاسوب، مدير دائرة الهندسة والصيانة والخدمات
وصف الخطر: يتمثّل هذا الخطر في التسرُّب المائيّ من الأنابيب أو الأدوار العُليا لمركز البيانات مما يسبّب غرق الأجهزة الخادمة لتقنية المعلومات وتلفها.		
نوع الخطر: وثائق ومعلومات		
احتمالية حدوث الخطر: ☐ عالي جدا ☐ عالي ☑ متوسط ☐ منخفض ☑ منخفض جداً		
تأثير الخطر حال حدوثه: ☐ شديد الخطورة ☐ خطير ☑ متوسط ☐ منخفض ☐ منخفض جداً		

سياسة درء الخطر:

1. عمل تفتيش دوريّ واختبارات على الأنابيب أو طرائق التسرُّب المائيّ لمنع حدوثها.
2. وضع اساليب ابتكاريّة لمنع تأثّر الأجهزة في حالة حدوث تسرُّب مائيّ.
3. تفعيل مركز بيانات مؤقّت في حالة حدوث تسرُّب مائيّ..

إجراء التعامل مع خطر التسرب المائي	
نوع الخطر:	التسرُّب المائيّ
مكان الخطر:	مركز الحاسوب
الشخص المسؤول (للاتصال به عند وقوع الخطر)	مدير مركز الحاسوب، مدير دائرة الهندسة والصيانة والخدمات
وسائل الاتصال به:	ايميل: compcenter@zuj.edu.jo maint@zuj.edu.jo هاتف 4291511 فرعي 200
الإجراء الفوري حال العلم بالخطر	الاتّصال بالمسؤول مباشرة
الجهة المسؤولة عن معالجة الخطر:	مركز الحاسوب، دائرة الهندسة والصيانة والخدمات

الإجراءات المتخذة لمعالجة الخطر:

1. إطفاء الأجهزة ومنع وصول الماء اليها.
2. البَدء بالبحث والتدقيق لتحديد مشكلة التسرُّب المائيّ.
3. حلّ المشكلة ومنع تكرار التسرُّب.
4. تشغيل الأجهزة وإعادة الوضع إلى ما كان عليه.
5. رفع تقرير الى رئاسة الجامعة عن المشكلة وكيفية حلّها، ومدى الضرر الحاصل، وتوعية المستخدِمِين والموظَّفِين.

انهاء الخطر والتخلص من الأضرار التي سببها:

إعادة البيانات إلى ما كانت عليه قبل التعطُّل عن طريق نُسَخ الأمان إذا كانت هناك أضرار في البيانات.

مخاطر الوثائق والمعلومات: خطر انقطاع الدّعم الفني والصيانة من مزودي الخدمات لمركز الحاسوب		
الخطر المتوقع	**بيانات الموقع**	**الشخص المسؤول**
مخاطر بيئة العمل: انقطاع الدَّعم الفنيّ والصيانة من المورِّد أو المقاول.	مركز الحاسوب المكان:جامعة الزيتونة الأردنية	الوظيفة: مدير مركز الحاسوب
وصف الخطر: يتمثَّل هذا الخطر في التوقُّف المفاجئ للدَّعم الفنيّ والصِّيانة للأجهزة أو أنظمة الاتّصالات من مزودي الخدمات لمركز الحاسوب.		
نوع الخطر: وثائق ومعلومات		
احتمالية حدوث الخطر: ☐ عالي جدا ☐ عالي ☑ متوسط ☐ منخفض ☑ منخفض جداً		
تأثير الخطر حال حدوثه: ☐ شديد الخطورة ☐ خطير ☑ متوسط ☐ منخفض ☐ منخفض جداً		

سياسة درء الخطر:

1. عمل دراسات معمّقة عن مزودي الخدمات لمركز الحاسوب قبل توقيع عقود الصيانة معهم.
2. توقيع عقود مع مزودي الخدمات لمركز الحاسوب بعد إستشارة جهة قانونية تابعة للجامعة وبشروط صارمة تحفظ مصالح الجامعة.
3. توافر بدائل ثانويّة لمحتوى التعاقد مع مزودي الخدمات لمركز الحاسوب قدر المستطاع .
4. المراجعة الدوريّة لأداء مزودي الخدمات لمركز الحاسوب ومقارنتها بالعقود الموقَّعة.

إجراء التعامل مع خطر انقطاع الدّعم الفني والصيانة من مزودي الخدمات لمركز الحاسوب	
نوع الخطر:	انقطاع الدَّعم الفنيّ والصيانة من مزودي الخدمات لمركز الحاسوب
مكان الخطر:	مركز الحاسوب
الشخص المسؤول (للاتصال به عند وقوع الخطر)	مدير مركز الحاسوب
وسائل الاتصال به:	ايميل: compcenter@zuj.edu.jo هاتف 4291511 فرعي 200
الإجراء الفوري حال العلم بالخطر	الاتّصال بالمسؤول مباشرة
الجهة المسؤولة عن معالجة الخطر:	مركز الحاسوب والمتشار القانوني للجامعة.

الإجراءات المتخذة لمعالجة الخطر:

1. استخدام بدائل للدَّعم الفنيّ من غير مزودي الخدمات لمركز الحاسوب.
2. رفع دعوى قضائيّة على مزودي الخدمات لمركز الحاسوب بالتعاون مع المتشار القانوني للجامعة.
3. توفير بدائل داخليّة للدَّعم الفنيّ.
4. رفع تقرير الى رئاسة الجامعة عن المشكلة وكيفية حلّها، ومدى الضَّرر الحاصل وتوعية المستخدِمِين والموظَّفِين.

انهاء الخطر والتخلص من الأضرار التي سببها:

1. عودة الخدمة الى سابق عهدها.
2. استمرارية الخدمة في البدائل المتاحة.

جدول تصنيف المخاطر (2017-2020)

احتمال حدوث الخطر: (5 عالي جداً)، (4 عالي)، (3 متوسط)، (2 منخفض)، (1 منخفض جداً)

تأثير الخطر عند حدوثه: (A شديد الخطورة)، (B خطير)، (C متوسط)، (D منخفض)، (E منخفض جداً)

الألوان: الأحمر (مستوى خطر مرتفع)، الأصفر (مستوى خطر متوسط)، الأخضر (مستوى خطر منخفض)

الرقم المتسلسل	رقم الخطر	الخطر	احتمال حدوث الخطر	تأثير الخطر عند حدوثه	تصنيف الخطر حسب مصفوفة المخاطر
ثالثاً: مخاطر الوثائق والمعلومات					
10	1	خطر الاختراق (Hacking)	منخفض	شديد الخطوره	2A
11	2	خطر الفيروسات	منخفض	خطير	2B
12	3	خطر الدّخول غير المُصرَّح به	منخفض جداً	خطير	1B
13	4	خطر استخدام النُّسخ غير الأصليّة من البرامج	منخفض	خطير	2B
14	5	خطر التّعديل غير المُصرَّح به للبيانات أو المعلومات	منخفض جداً	خطير	1B
15	6	خطر دقّة البيانات والمعلومات وتوافقها وتكاملها	منخفض جداً	متوسط	1C
16	7	خطر أعطال الأجهزة أو البرامج	منخفض	متوسط	2C
17	8	خطر فقْد البيانات بسبب الفيضانات أو الحرائق أو الزلازل أو البراكين أو الحروب	منخفض جداً	متوسط	1C
18	9	خطر سرقة الخوادم وأجهزة التخزين	منخفض جداً	شديد الخطوره	1A
19	10	خطر نقص المهارات والكفاءات	متوسط	متوسط	3C
20	11	خطر الأخطاء البشريّة (Human Errors)	منخفض	منخفض	2D
21	12	خطر انقطاع التيار الكهربائي	متوسط	منخفض	3D
22	13	خطر انقطاع التكييف	منخفض جداً	متوسط	1C
23	14	خطر التسرُّب المائيّ	منخفض جداً	متوسط	1C
24	15	خطر انقطاع الدَّعم الفنيّ والصيانة من مزودي الخدمات لمركز الحاسوب	منخفض جداً	متوسط	1C