

جامعة الأميرة
نورة بنت عبدالرحمن



سياسة التخزين والاستبقاء

المملكة العربية السعودية
وزارة التعليم
جامعة الأميرة نورة بنت عبدالرحمن
اللجنة التوجيهية للحوكمة والالتزام وإدارة
المخاطر والطوارئ واستمرارية الأعمال

جدول المحتويات

٤.....	١. المقدمة
٤.....	١.١. جدول التعريفات
٦.....	١.٢. الغرض
٦.....	١.٣. النطاق
٦.....	١.٤. المستند النظامي
٧.....	٢. بيان السياسة
٧.....	٢.١. المبادئ التوجيهية لتخزين البيانات واستبقائها
٧.....	٢.٢. شروط تخزين البيانات
٨.....	٢.٣. استبقاء البيانات
٩.....	٢.٤. أرشفة البيانات
٩.....	٢.٥. قواعد حذف البيانات
١٠.....	٢.٦. النسخ الاحتياطي للبيانات واسترجاعها
١٠.....	٢.٧. التعافي من الكوارث
١٠.....	٢.٨. فقدان البيانات غير المقصود
١٢.....	٣. الأدوار والمسؤوليات
١٣.....	٤. المراجعة والتحديث
١٣.....	٥. الامتثال
١٣.....	٦. التواصل
١٣.....	٧. السياسات ذات العلاقة

معلومات الوثيقة:

اسم الوثيقة	سياسة التخزين والاستبقاء
نوع الوثيقة	سياسة
مالك الوثيقة	مكتب إدارة البيانات
تاريخ الإعداد	١٤٤٧/٠٤/٣٣ هـ
تصنيف الوثيقة	مقيّد - داخلي
النسخة رقم	١,٠

إصدارات الوثيقة:

تاريخ الإصدار	معد الوثيقة	الإصدار	التغييرات بالوثيقة
١٤٤٧/٨/٢٤ هـ	مكتب إدارة البيانات	١,٠	

مراجعات الوثيقة:

التاريخ	الجهة	ملاحظات
١٤٤٧/٧/٤ هـ	إدارة الأمن السيبراني	
١٤٤٧/٧/١٦ هـ	الإدارة العامة للحوكمة والمخاطر والالتزام	
١٤٤٧/٨/١٦ هـ	الإدارة القانونية	

اعتماد الوثيقة:

التاريخ	الجهة	الختم



١. المقدمة

تحرص جامعة الأميرة نورة بنت عبد الرحمن إلى وضع إطار منظم لإدارة دورة حياة البيانات داخل الجامعة، يشمل ضوابط حفظها وتخزينها وأرشفتها وحذفها بشكل آمن ومتوافق مع المعايير الوطنية وذلك بناءً على الفقرة (أ) من البند (عاشراً) من قرار مجلس الوزراء رقم (٢٩٢) وتاريخ ١٤٤٧/٤/٢٧هـ، الذي أسند إلى مكتب إدارة البيانات الوطنية مهمة وضع السياسات وآليات الحوكمة والمعايير والضوابط الخاصة بالبيانات والتحقق من مدى امتثال الجهات لها. كما تركز السياسة على حماية البيانات من فقدان أو الوصول غير المصرح به، ودعم استمرارية الأعمال من خلال النسخ الاحتياطي والتعافي من الكوارث، إضافة إلى تعزيز كفاءة التخزين والامتثال وتمكين اتخاذ القرار المبني على بيانات موثوقة.

١.١. جدول التعريفات

يُقصد بالمصطلحات الواردة أدناه - أينما وردت في هذه السياسة - المعاني الموضحة أمام كل منها، ما لم يقتض سياق النص خلاف ذلك:

المصطلح	الوصف
الجامعة	جامعة الأميرة نورة بنت عبد الرحمن.
جهات الجامعة	الوحدات التنظيمية بالجامعة بما فيها مستشفى الملك عبد الله بن عبد العزيز الجامعي.
اللجنة التوجيهية لإدارة وحوكمة البيانات	هي لجنة عليا داخل الجامعة مكلفة بالإشراف الاستراتيجي على إدارة البيانات وحوكمتها.
المكتب	مكتب إدارة البيانات في جامعة الأميرة نورة بنت عبد الرحمن.
البيانات	مجموعة من الحقائق في صورتها الأولية أو في صورة غير منظمة مثل الأرقام أو الحروف أو الصور الثابتة أو الفيديو أو التسجيلات الصوتية أو الرموز التعبيرية.
إدارة البيانات	عملية تطوير الخطط والسياسات والبرامج والممارسات وتنفيذها والإشراف عليها لتمكين الجامعة من حوكمة البيانات وتعزيز قيمتها باعتبارها أحد الأصول القيمة والثمينة.
تخزين البيانات	آلية حفظ البيانات على أجهزة ووسائل تخضع للتدابير اللازمة لتوفير البيانات بسهولة.
استبقاء البيانات	هو حفظ البيانات في بيئة إنتاج أو بيئة فعلية خلال "فترة الاستخدام النشط لها" بحيث يمكن الوصول إليها من قبل المستخدم المصرح له في إطار أنشطته العادية.
أرشفة البيانات	عملية نقل البيانات التي لم تعد مستخدمة على نحو فعال إلى جهاز تخزين منفصل للحفاظ طويل الأجل بحيث تتألف بيانات الأرشفة من بيانات قديمة لا تزال مهمة للجامعة وقد تكون مطلوبة للرجوع إليها في المستقبل وبيانات يجب الاحتفاظ بها للالتزام بالتشريعات والتنظيمات ذات العلاقة.

المصطلح	الوصف
النسخ الاحتياطي	الملفات والأجهزة والبيانات والإجراءات المتاحة للاستخدام في حالة الأعطال أو فقدان أو إذا حُذف الأصل منها أو توقف عن الخدمة.
الأنظمة الحساسة	هي أي أنظمة أو شبكات يؤدي تعطيلها أو التغيير غير المشروع لطريقة عملها أو الدخول غير المصرّح به إليها أو إلى البيانات والمعلومات التي تحفظها أو تعالجها إلى تأثير سلبي على توافر الخدمات أو أعمال الجامعة أو التسبب في آثار اقتصادية أو مالية أو أمنية على المستوى الوطني.
التعافي من الكوارث	الإجراءات والخطط التي تضعها الجامعة لضمان استمرار عمل أنظمتها وبياناتها بعد حدوث كارثة أو أزمة كبيرة، سواء كانت طبيعية أو بشرية أو تقنية.
مبدأ الحد الأدنى من الامتيازات	تُقيد إدارة صلاحيات العاملين إلى الحد الأدنى من الامتيازات اللازمة لأداء المهام والمسؤوليات المسندة إليهم.
مبدأ الحاجة إلى المعرفة	يُقيد الوصول إلى البيانات واستخدامها على أساس الاحتياج الفعلي للمعرفة ولأقل عدد ممكن من العاملين.
ممثّل بيانات الأعمال	الشخص المسؤول عن البيانات التي تجمعها الجامعة أو تحتفظ بها داخل إدارته، وعادةً ما يكون في مستوى إداري عالٍ.
مختص بيانات الأعمال	شخص يرشحه ممثّل بيانات الأعمال، ويكون خبيرًا بمجال معين ويتولى تطبيق سياسات ومعايير إدارة البيانات داخل الإدارة الخاصة به.
تقني وفني البيانات	شخص تقني مسؤول عن تنفيذ ضوابط حوكمة البيانات وتطبيقها على قواعد البيانات والأنظمة بالتعاون مع مختصي البيانات.

١,٢. الغرض

تهدف هذه السياسة إلى حماية البيانات من فقدان أو الوصول غير المصرح به، وضمان جاهزيتها واستمراريتها لدعم العمليات الأكاديمية والإدارية، مع تعزيز الكفاءة والامتثال وتمكين اتخاذ القرار المبني على بيانات موثوقة.

١,٣. النطاق

تُطبق أحكام هذه السياسة على جميع البيانات التي تتلقاها الجامعة أو تنتجها أو تتعامل معها، شريطة أن تكون مخزنة أو مُعالجة إلكترونياً، وتشمل البيانات الموجودة في قواعد البيانات والأنظمة التشغيلية والتطبيقات ورسائل البريد الإلكتروني ووسائل التخزين الإلكترونية والسجلات الرقمية والملفات الصوتية والمرئية والصور الرقمية وجميع أشكال البيانات الإلكترونية الأخرى.

١,٤. المستند النظامي

- ضوابط ومواصفات إدارة البيانات الوطنية وحكمتها وحماية البيانات الشخصية الصادرة من مكتب إدارة البيانات الوطنية - إصدار ١,٥ عام ٢٠٢١م.
- الهيئة الوطنية للأمن السيبراني (NCA)، ضوابط الأمن السيبراني.
- الضوابط الأساسية للأمن السيبراني (Essential Cybersecurity Controls ECC).
- ضوابط حماية البيانات (Data Cybersecurity Controls DCC).



٢. بيان السياسة

٢.١ المبادئ التوجيهية لتخزين البيانات واستبقائها

٢.١.١ الموثوقية

التأكد من موثوقية وسائل تخزين البيانات وكفاءتها من خلال مراقبة أدائها بصورة دورية والإبلاغ الفوري عن أي مشاكل قد تؤثر على سلامة البيانات أو توافرها.

٢.١.٢ الإتاحة

تخزين البيانات باستخدام أفضل الأدوات والمنهجيات لضمان أعلى مستويات الإتاحة للبيانات في الظروف التشغيلية الاعتيادية أو أثناء الحالات الحرجة.

٢.١.٣ القدرة على الاستعادة

عدم الاعتماد على مخزن واحد للبيانات، مع ضمان وجود نسخ احتياطية محدثة تُمكن من استعادة البيانات على نحو آمن وسريع عند الحاجة بما يضمن استمرارية أعمال الجامعة.

٢.١.٤ اعتبارات حساسية الأنظمة

اتباع أفضل الممارسات والإجراءات الأمنية المعتمدة عند تخزين بيانات الأنظمة الحساسة أو التخلص منها، مع تطبيق ضوابط الوصول استنادًا إلى مبادئ "الحد الأدنى من الامتيازات" و"الحاجة إلى المعرفة".

٢.١.٥ الحفظ والاستبقاء

وضع معايير واضحة لمدة حفظ البيانات وفقًا لمتطلبات تنظيمية بالإضافة إلى حساسيتها بالنسبة للأعمال، مع إتاحة إتلاف البيانات بأمان عند انتهاء مدة الاستبقاء.

٢.١.٦ الكفاءة والتكلفة

تحقيق التوازن بين كفاءة عمليات تخزين البيانات والتكاليف المرتبطة بها بما يضمن الاستخدام الأمثل للموارد المتاحة.

٢.٢ شروط تخزين البيانات

٢.٢.١ تنفيذ عمليات تخزين البيانات وفقًا لأفضل الممارسات والمعايير المعتمدة بما يضمن سلامتها وسهولة الوصول إليها عند الحاجة.

٢.٢.٢ عند تخزين البيانات يتم اتباع القواعد الصادرة من الهيئة الوطنية للأمن السيبراني والتي تشمل:

- **البيانات المصنفة "عام"**: الالتزام بمتطلبات الضوابط الأساسية للأمن السيبراني بهذا الخصوص.
- **البيانات المصنفة "مقيّد"**: بالإضافة إلى إرشادات الحد الأدنى في "عام"، تُطبق القواعد الآتية:
- تُحفظ البيانات المصنفة في أجهزة تابعة للجامعة أو الأجهزة المصرّح لها من خارج الجامعة.
- تشفير وسائط الحفظ والتخزين المتنقلة عند استخدامها.
- عند المشاركة، يجب استخدام طرق وخوارزميات محدثة وآمنة للتشفير على مستوى جميع وسائل وأنشطة الاتصال الشبكي المستخدم لنقل البيانات وفقًا للمستوى المتوسط ضمن المعايير الوطنية للتشفير الموضحة في ضوابط الأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني.
- **البيانات المصنفة "سري"**: بالإضافة إلى إرشادات الحد الأدنى في "مقيّد"، تُطبق القواعد الآتية:
- تُحفظ البيانات المصنفة في أجهزة تابعة للجامعة.
- تُشفّر البيانات الموضوعة تحت هذا التصنيف تشفيرًا دائمًا عند الحفظ إلكترونيًا وفقًا للمستوى المتقدم ضمن المعايير الوطنية للتشفير الموضحة في ضوابط الأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني.

- أخذ موافقة صاحب الصلاحية قبل استخدام وسائط حفظ البيانات والتخزين المتنقل لها وتشفيرها.
- يجب أن يكون تخزين البيانات داخل الجامعة أو في خدمات الحوسبة السحابية المقدمة من جهات داخل المملكة العربية السعودية.
- **البيانات المصنفة "سري للغاية":** بالإضافة إلى إرشادات الحد الأدنى في "سري"، تُطبق القواعد الآتية:
 - لا يسمح بتخزين البيانات المصنفة بـ«سري للغاية» في الخدمات السحابية.
- ٢.٢.٣. التخطيط لإجراء النسخ الاحتياطي وفق منهجية موحدة تعتمد على أولويات ومتطلبات الأعمال، على أن تشمل الخطة مواعيد النسخ الاحتياطي وآلية تسجيله ومكان الاحتفاظ به وأسس التسمية والعنونة.
- ٢.٢.٤. التأكد من أن البيانات محمية بجدول نسخ احتياطي مناسب ومن إمكانية استعادتها عند الحاجة.
- ٢.٢.٥. تفعيل اتفاقيات مستوى الخدمة الخاصة بأداء قواعد البيانات وتنفيذ هذه الاتفاقيات بحيث تحدد متطلبات الجامعة لأداء قواعد البيانات وتوفر البيانات واستعادتها، وتشمل الإطار الزمني لإتاحة قاعدة البيانات للمستخدمين وأقصى زمن مسموح به لإنجاز العمليات الإلكترونية لتطبيق معين وإجراءات التصعيد الواجب اتخاذها عند مخالفة اتفاقية مستوى الخدمة.
- ٢.٢.٦. تحديد متطلبات الأمن السيبراني الخاصة بإدارة النسخ الاحتياطية في الجامعة وتوثيق تلك المتطلبات وتطبيقها. ويجب أن تغطي هذه المتطلبات، كحد أدنى، ما ورد ضمن وثيقة "الضوابط الأساسية للأمن السيبراني" الصادرة عن الهيئة الوطنية للأمن السيبراني، وتشمل:
 - نطاق النسخ الاحتياطية وشموليتها للأصول المعلوماتية والتقنية الحساسة.
 - القدرة السريعة على استعادة البيانات والأنظمة بعد التعرض لحوادث الأمن السيبراني.
 - إجراء فحص دوري لمدى فعالية استعادة النسخ الاحتياطية.
 - عمل النسخ الاحتياطي على فترات زمنية مخطط لها بناءً على تقييم المخاطر للجامعة. ويفضل عمل النسخ الاحتياطي، للأنظمة الحساسة، بصورة يومية.
 - تأمين الوصول لمحتوى النسخ الاحتياطية للأنظمة الحساسة ووسائطها وتأمين تخزين هذا المحتوى ونقله، وحماية هذه النسخ من الإتلاف أو التعديل أو الاطلاع غير المصرح به.
- ٢.٢.٧. الاحتفاظ بسجلات الأحداث السيبرانية لمدة لا تقل عن اثني عشر (١٢) شهرًا للأنظمة العامة وثمانية عشر (١٨) شهرًا للأنظمة الحساسة كحد أدنى، مع ضمان توافق ذلك مع السياسات الداخلية والمتطلبات التشريعية والتنظيمية ذات العلاقة.
- ٢.٢.٨. تحديد السعة التخزينية المتوقعة للبيانات لكل نظام أو تطبيق بناءً على دراسة السعات المستخدمة سابقًا وتقييم أداء الأنظمة والتطبيقات ورفع تقرير شامل بذلك إلى مكتب إدارة البيانات يتضمن توقع الاحتياجات المستقبلية وتقديرات لميزانية عمليات الشراء المستقبلية لدراساتها وإبداء المرنّيات عليها.
- ٢.٢.٩. إنشاء سجل لمؤشرات الأداء الرئيسية لتخزين البيانات واستبقائها لقياس التقدم المحرز في خطة تخزين البيانات.

٢.٣. استبقاء البيانات

- ٢.٣.١. يتولى ممثل بيانات الأعمال المسؤول عن الإدارة أو القسم المعني إعداد جدول زمني يحدد فترات استبقاء جميع البيانات ومراجعتها بصورة دورية أو عند حدوث أي تغييرات في المتطلبات ذات العلاقة.
- ٢.٣.٢. تُحدد فترة الاستبقاء لكل نوع من أنواع البيانات وفقًا لما يلي:
 - **بيانات دائمة الحفظ – بيانات حيوية:** وهي البيانات التي لا يمكن الاستغناء عنها ويجب توفرها دائمًا لأداء أعمال الجامعة اليومية مثل: البيانات المالية والبيانات الأكاديمية والبيانات البحثية. وتُحدد مدة استبقاء هذه البيانات وفقًا لطبيعتها وأهميتها.

- **بيانات مؤقتة الحفظ - بيانات غير حيوية:** وهي البيانات التي تُستخدم لفترة محددة ولا توجد حاجة للرجوع إليها بعد فترة الاحتفاظ (إذ من المقترح التخلص من البيانات المؤقتة على نحو ربع سنوي).
٢,٣,٣. عدم استبقاء البيانات المستخدمة في العمل المؤقت أو التطوير أو الاختبار أو مسودات البيانات إلى ما بعد فترة استخدامها النشط ولا ينبغي نسخها في بيانات الإنتاج أو البيانات الفعلية.

٢,٤. أرشفة البيانات

٢,٤,١. مدة أرشفة البيانات ٥ سنوات، ما لم يحدد ممثل بيانات الأعمال خلاف ذلك، بناء على متطلب نظامي أو أعمال. وينبغي على ممثل بيانات الأعمال التشاور مع مكتب إدارة البيانات والحصول على الاستشارات منه، عند اللزوم، لتوضيح اختياره لفترة الاحتفاظ.
٢,٤,٢. إعداد قائمة مفصلة تتضمن المستخدمين المصرّح لهم بالوصول إلى البيانات المؤرشفة وتوثيق تلك القائمة.
٢,٤,٣. تتحمل إدارة تقنية المعلومات والاتصالات مسؤولية تنفيذ إجراءات أتمتة الأرشفة للبيانات بعد انتهاء فترة الاحتفاظ بها.
٢,٤,٤. تتحمل إدارة تقنية المعلومات والاتصالات مسؤولية تنفيذ فترة الأرشفة المعتمدة للبيانات وفق ما أقره ممثل بيانات الأعمال وضمان تطبيقها بما يتوافق مع السياسات والإجراءات المعتمدة في الجامعة.
٢,٤,٥. أرشفة البيانات في مواقع تضمن حماية سرّيتها وسلامتها وتُمكن من الوصول إليها عند الحاجة بطريقة آمنة ومنظمة.
٢,٤,٦. عند أرشفة البيانات اتباع القواعد الصادرة عن الهيئة الوطنية للأمن السيبراني.
٢,٤,٧. تُحدد مدد الأرشفة والاستبقاء لكل نوع من أنواع البيانات وفق التصنيف المذكور بقسم استبقاء البيانات في هذه السياسة.
٢,٤,٨. بعد انتهاء فترة الأرشفة، ينبغي إتلاف البيانات وفقاً لما هو منصوص عليه في قسم التخلص من البيانات.

٢,٥. قواعد حذف البيانات

٢,٥,١. تتولى إدارة تقنية المعلومات والاتصالات بالتنسيق مع إدارة الأمن السيبراني تحديد قائمة مفصلة بطرق الإتلاف الآمنة والمعتمدة وتنفيذها لكل نوع من البيانات المؤرشفة، سواء كانت مخزنة على وسائط مادية مثل الأقراص الصلبة أو الأقراص المدمجة أو أشرطة النسخ الاحتياطية أو الأجهزة المحمولة أو محركات الأقراص المتنقلة أو كانت ضمن سجلات قواعد البيانات أو ملفات النسخ الاحتياطية.
٢,٥,٢. يتولى مكتب إدارة البيانات مراجعة إجراءات التخلص من البيانات بعد انتهاء فترة الأرشفة وتقديم التوصيات اللازمة بشأنها.
٢,٥,٣. عند حذف أو إزالة البيانات بالالتزام بالقواعد الصادرة عن الهيئة الوطنية للأمن السيبراني، والتي تشمل على سبيل المثال لا الحصر ما يلي:
- **البيانات المصنفة "عام":** يجب الالتزام بمتطلبات الضوابط الأساسية للأمن السيبراني بهذا الخصوص.
- **البيانات المصنفة "مقيّد":** بالإضافة إلى إرشادات الحد الأدنى في "عام"، تُطبق القواعد الآتية:
- عند الحاجة إلى إعادة استخدام أجهزة التخزين، تُحذف البيانات السابقة من أجهزة التخزين عن طريق خاصية الطمس.
- عند عدم الحاجة إلى إعادة استخدام أجهزة التخزين، يتم التخلص من أجهزة التخزين عن طريق الإتلاف الكامل.
- **البيانات المصنفة "سري" أو "سري للغاية":** بالإضافة إلى إرشادات الحد الأدنى في "مقيّد"، تُطبق القواعد الآتية:
- التخلص من أجهزة التخزين عن طريق الإتلاف الكامل في حال الانتهاء من استخدام أجهزة التخزين.
- توثيق عملية الإتلاف بمحضر.

٢,٥,٤. تتولى إدارة تقنية المعلومات والاتصالات مسؤولية تنفيذ إجراءات التخلص من البيانات وفقاً للضوابط المعتمدة.
٢,٥,٥. إلتلاف البيانات عند انتهاء مدة الاستبقاء المحددة لها أو عند عدم الحاجة التشغيلية لها أو بعد انتهاء الغرض الذي جُمعت من أجله، وذلك وفق الضوابط المعتمدة وباستخدام طرق تضمن عدم إمكانية استرجاعها، مع توثيق عملية الإلتلاف بالكامل.

٢,٦. النسخ الاحتياطي للبيانات واسترجاعها

يجب وضع عملية واضحة للنسخ الاحتياطي للبيانات واسترجاعها والالتزام بهذه العملية، وتشمل ما يلي:
٢,٦,١. تحديد تواتر إجراء النسخ الاحتياطي لكل نظام معلومات في الجامعة وفقاً لأهمية النظام وحساسية البيانات ومتطلبات العمل التشغيلية.
٢,٦,٢. تحديد نطاق النسخ الاحتياطي لكل نظام معلومات ويشمل نطاق البيانات ونطاق سجل معاملات قاعدة البيانات.
٢,٦,٣. تحديد موقع الملفات الاحتياطية ويشمل وسيط التخزين والموقع المادي لمخزن البيانات.
٢,٦,٤. التحقق الدوري من اكتمال النسخ الاحتياطي.

٢,٧. التعافي من الكوارث

تتولى إدارة تقنية المعلومات والاتصالات وضع خطة للتعافي من الكوارث، وذلك بالتعاون مع مكتب إدارة البيانات، على أن تشمل ما يلي:
٢,٧,١. قائمة أولويات بأنظمة المعلومات تُستخدم لتحديد تسلسل استرجاعها أثناء تنفيذ خطط التعافي من الكوارث.
٢,٧,٢. تخصيص الأدوار والمسؤوليات المتعلقة بالتعامل مع حالات الاستجابة للحوادث.
٢,٧,٣. تحديد الإجراءات الواجب اتباعها لتفعيل نظام الاستجابة للحوادث.
٢,٧,٤. تحديد الإجراءات الواجب اتخاذها لتقليل الأضرار وتخفيف عواقب الحوادث في العمليات الحيوية داخل الجامعة.
٢,٧,٥. تحديد أهداف نقطة التعافي لكل نظام معلومات مذكور في الخطة.
٢,٧,٦. تحديد أنشطة وإجراءات التعافي المطلوبة لكل نظام معلومات.

٢,٨. فقدان البيانات غير المقصود

٢,٨,١. في حال فقدان البيانات على نحو دائم (غير مقصود)، يتولى ممثل بيانات الأعمال إعداد بلاغ رسمي وتوجيهه إلى إدارة تقنية المعلومات والاتصالات لاتخاذ الإجراءات اللازمة على أن يتضمن هذا البلاغ تفاصيل البيانات المفقودة وسبب الحاجة إليها وأسباب الفقدان والعامل أو الجهة المسؤولة، بالإضافة إلى التوقيت الزمني والأجهزة أو الأنظمة ذات العلاقة.
٢,٨,٢. تتولى إدارة تقنية المعلومات والاتصالات تحليل حادثة فقدان البيانات وتوجيهها إلى إدارة الأمن السيبراني إذا كانت الحادثة ناتجة عن اختراق أمني، إضافةً إلى محاولة استعادة البيانات من الأنظمة أو الأجهزة التي فُقدت عليها البيانات باستخدام أفضل التقنيات والأدوات المعتمدة.
٢,٨,٣. في حال عدم التمكن من استعادة البيانات من الأنظمة أو الأجهزة، يتعين على إدارة تقنية المعلومات والاتصالات البحث عن البيانات المطلوبة في النسخ الاحتياطية التي جرى إنشاؤها مسبقاً.
٢,٨,٤. يتعين على إدارة تقنية المعلومات والاتصالات تنفيذ عملية استرجاع البيانات من النسخ الاحتياطية على نحو كامل والتحقق من صلاحية هذه البيانات على البيئة التجريبية قبل نقلها إلى البيئة التشغيلية.
٢,٨,٥. يتولى مكتب إدارة البيانات - بالتعاون مع ممثلي بيانات الأعمال المعنيين - تقييم أهمية وحجم البيانات المفقودة استناداً إلى تصنيفها ومدى تأثير فقدانها على أعمال الجامعة.

٢٨٦. إذا كانت البيانات ذات أهمية عالية وحجمها كبيرًا، تتولى اللجنة التوجيهية لحوكمة البيانات في الجامعة مراجعة حالة فقدان البيانات والتوجيه بتنفيذ الإجراءات اللازمة.

٢٨٧. يتولى مكتب إدارة البيانات إعداد تقرير بحادثة فقدان البيانات بما يشمل استخراج الدروس المستفادة من الإجراءات الاحتياطية والرفع بها إلى اللجنة التوجيهية لإدارة وحوكمة البيانات في الجامعة والتي تشترع بدورها في اعتمادها.



٣. الأدوار والمسؤوليات

الدور	المسؤولية
اللجنة التوجيهية لإدارة وحكومة البيانات	- التوصية باعتماد السياسة.
اللجنة التوجيهية للحكومة والالتزام وإدارة المخاطر والطوارئ واستمرارية الأعمال	- اعتماد السياسة.
مكتب إدارة البيانات	- الإشراف على تنفيذ السياسة عبر مختلف جهات الجامعة. - مراقبة الامتثال على مستوى جهات الجامعة لعملية تخزين البيانات واستبقائها ومدى فعاليتها. - مراجعة إجراءات التخلص من البيانات بعد انتهاء فترة الأرشفة وتقديم التوصيات اللازمة بشأنها. - تقييم أهمية وحجم البيانات المفقودة وتأثيرها على أعمال الجامعة بالتعاون مع ممثلي بيانات الأعمال.
إدارة تقنية المعلومات والاتصالات	- الالتزام بعملية واضحة لمنح صلاحية الوصول إلى قواعد البيانات وحفظ سجلات الدخول للبيانات. - إنشاء خطة للتعافي من الكوارث، وذلك بالتعاون مع مكتب إدارة البيانات. - تحديد السعة التخزينية لكل نظام ورفع تقرير بالاحتياجات المستقبلية والميزانية لمكتب إدارة البيانات.
إدارة الأمن السيبراني	- ضمان تنفيذ الضوابط الأمنية لحماية البيانات وفقاً للوائح الهيئة الوطنية للأمن السيبراني وبالمواءمة مع مكتب إدارة البيانات.
ممثل بيانات الأعمال	- يمثل المركز في تحديد متطلبات الأعمال المتعلقة بتخزين البيانات وفترات الاحتفاظ بها. - ضمان مواءمة الأعمال مع اللوائح التنظيمية بالتعاون مع الجهات ذات العلاقة. - تحديد فترات الأرشفة والاستبقاء المطلوبة للبيانات.
مختص بيانات الأعمال	- تحديد مدى أهمية الأنظمة المتعلقة بالأعمال المهمة، وذلك لتحديد أولوية نظم المعلومات في حالات التعافي من الكوارث.

٤. المراجعة والتحديث

- ٤,١. يجب مراجعة هذه السياسة من قبل المكتب دوريًا، أو عند وجود متطلبات جديدة تستوجب التعديل.
- ٤,٢. يجب مشاركة التحديثات المقترحة مع الجهات المعنية داخل الجامعة لأغراض المراجعة.
- ٤,٣. يجب تنفيذ التعديلات من قبل المكتب ورفع النسخة النهائية إلى اللجنة التوجيهية للحوكمة والالتزام وإدارة المخاطر والطوارئ واستمرارية الأعمال لاعتمادها.

٥. الامتثال

- ٥,١. يجب على جميع جهات الجامعة ضمان تطبيق هذه السياسة والالتزام ببندوها حيث يقوم المكتب بمراجعة دورية أو عشوائية للتحقق من الامتثال لها.
- ٥,٢. عند مراجعة حالات عدم الامتثال، يتبع المكتب منهجية تدريجية لتحليل سبب عدم الامتثال ومدى الآثار والمخاطر المترتبة على ذلك، حسب الإجراءات التنظيمية المتبعة في مكتب إدارة البيانات.

٦. التواصل

- في حال وجود أي استفسارات يرجى التواصل مع مكتب إدارة البيانات في جامعة الأميرة نورة بنت عبد الرحمن - بريد إلكتروني: (DMO@pnu.edu.sa).

٧. السياسات ذات العلاقة

- ٧,١. سياسة حماية البيانات الشخصية.
- ٧,٢. سياسة حوكمة البيانات.
- ٧,٣. سياسة تصنيف البيانات.

انتهى

المملكة العربية السعودية

وزارة التعليم

جامعة الأميرة نورة بنت عبد الرحمن

اللجنة التوجيهية للحوكمة والالتزام وإدارة
المخاطر والطوارئ واستمرارية الأعمال





جامعة الأميرة نورة بنت عبد الرحمن
Princess Nourah Bint Abdulrahman University