جامعة الحدود الشمالية
NORTHERN BORDER UNIVERSITY
مكتب إدارة البيانات

رؤية VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

V1.0

دليل التوعية بحماية البيانات الشخصية

#بياناتك_حياتك

المحتويات

لماذا نهتم بحماية البيانات الشخصية؟

في عالم رقمي متزايد، تصبح حماية البيانات الشخصية ضرورة، ليس فقط للأفراد بل أيضاً للمؤسسات وكذلك الحماية من الجهات التي قد تستخدمها بطرق غير أخلاقية

وفي الجامعة

حماية البيانات تكتسب أهمية خاصة بسبب تنوع المعلومات المحفوظة. مثل بيانات الموظفين والطلاب. أي تسريب أو تلاعب يمكن أن يؤثر سلباً على سمعة الجامعة.

هدف الدليل

يهدف هذا الدليل إلى توعية الأفراد بأهمية حماية البيانات الشخصية ومساعدتهم على اتخاذ التدابير الوقائية اللازمة لضمان خصوصيتهم وأمان بياناتهم

ما هي البيانات الشخصية؟

البيانات الشخصية هي المعلومات التي تمكن من التعرف على الفرد سواء كان ذلك مباشرة أو غير مباشرة، مثل الاسم أو رقم الهوية.

أنواع البيانات الشخصية

1- بيانات تعريفية:	2- بيانات ديموغرافية:	3- بيانات طبية:	4- بيانات مالية:
تشمل الاسم، رقم الهوية والبريد الإلكتروني	تضم العمر، الجنس والجنسية	تشمل التأمين الصحي والسجل	مثل رقم الحساب البنكي والتفاصيل

البيانات الشخصية الحساسة

هي البيانات التي تحتاج إلى مستوى عال من الحماية، مثل البيانات الطبية أو البيانات التي تكشف عن العرق أو المعتقدات الدينية.

الوصول إلى البيانات

القدرة على الوصول المنطقي والمادي إلى بيانات الجهة وموارداها الفنية لغرض استخدامها.

مستويات تصنيف البيانات

تصنيف البيانات في فئات وفق مستوى السرية والأهمية إلى: سري للغاية، سري، مقيد، وعام.

مبادئ حماية البيانات الشخصية

الخصوصية

حق الفرد في التحكم بالبيانات ومن يمكنه الوصول إليها.

النزاهة

ضمان دقة البيانات وحمايتها من التحريف.

الموثوقية

القدرة على مشاركة البيانات بين نظم مختلفة مع مراعاة الأمان.

الأمان

وجود إجراءات لمنع الوصول لغير المصرح به للبيانات.

المساءلة

وجود آليات لمحاسبة المسؤولين عن أي انتهاكات.

الشفافية

إبلاغ الأفراد عن جمع واستخدام بياناتهم.

نظام حماية البيانات الشخصية

مقدمة عن النظام

نظام حماية البيانات الشخصية، هو تشريع أخذ النفاذ في المملكة العربية السعودية منذ 24 سبتمبر 2023، وهو ينظم كيفية معالجة البيانات الشخصية للأفراد المقيمين في المملكة.

النطاق

يغطي نظام حماية البيانات الشخصية كل الشركات والمؤسسات التي تعمل داخل المملكة وخارجها والتي تقدم خدمات لمواطنيها والمقيمين فيها.

الأهداف

1- حماية البيانات الشخصية وخصوصية الأفراد.

2- ضمان الشفافية في معالجة البيانات.

3- توفير وسائل لمحاسبة المؤسسات في حالة المخالفات.

حقوق الأفراد

1- الحق في الوصول للبيانات.

2- الحق في النسيان.

3- الحق في التصحيح.

4- الحق في الاعتراض على معالجة البيانات.

التأثير على الجامعات

الجامعات التي تتعامل مع بيانات مواطني المملكة والمقيمين فيها يجب عليها الامتثال لأحكام النظام، وذلك يشمل بيانات الطلاب والباحثين والموظفين.

المخالفات والعقوبات

عدم الامتثال لأحكام النظام يمكن أن يؤدي إلى عقوبات مالية كبيرة، بالإضافة إلى تأثير سبي على سمعة المؤسسة.

سياسة حماية البيانات الشخصية

تمت الموافقة على وثيقة سياسة البيانات الشخصية بجامعة الحدود الشمالية من قبل معالي الجامعة. تحدد السياسة التعريفات والأهداف ونطاق التطبيق والامتثال للسياسة والمبادئ الرئيسية لحماية البيانات الشخصية بجامعة الحدود الشمالية وبنود السياسة والوثائق ذات الصلة.

النطاق

تنطبق هذه السياسة على الجهات الجامعية التي تتعامل مع البيانات الشخصية لمنسوبي الجامعة ومن يرتبط بها بعلاقة تعاقدية أو تنظيمية، ولا تنطبق عند الوفاء بالالتزامات التنظيمية أو القضائية أو الإلزامية.

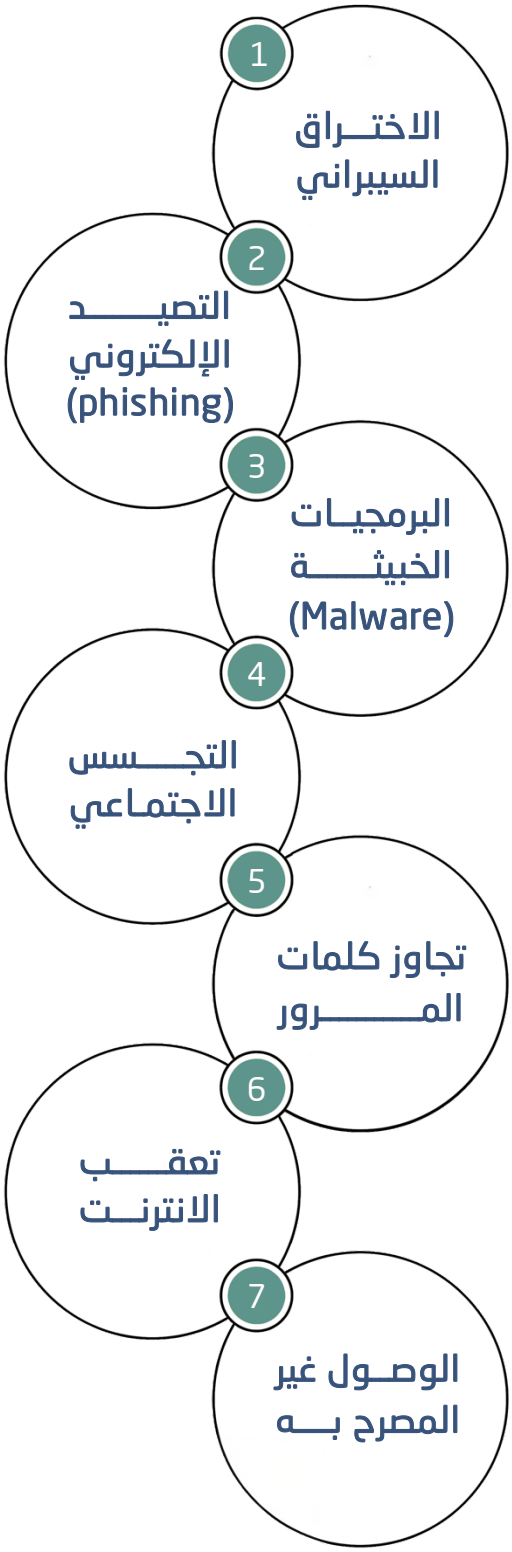
الأهداف

- تحديد متطلبات حماية البيانات الشخصية بجامعة الحدود الشمالية.
- تلتزم بالمتطلبات التشريعية في الوثيقتين.
- ضوابط إدارة البيانات الشخصية وحوكمتها وحماية البيانات الشخصية (الإصدار: يناير 2021) وسياسات حوكمة البيانات الوطنية (الإصدار الثاني: مايو 2021).

حقوق الأفراد

1. الحق في العلم بالمستند النظامي والغرض من جمع بياناتهم.
2. الحق في الرجوع عن موافقته على معالجة بياناته.
3. الحق في الوصول إلى بياناته الشخصية وطلب تصحيحها.

التهديدات الشائعة



هو استغلال الثغرات الأمنية للوصول إلى البيانات الشخصية دون إذن.

هي عمليات تستهدف الحصول على بيانات شخصية عبر إرسال رسائل إلكترونية مزيفة تبدو وكأنها من مصادر موثوقة.

برامج مصممة للتسلل والسيطرة على الأجهزة، وقد تستخدم لسرقة البيانات الشخصية.

تقنيات تستخدم لاستغلال الناس للكشف عن معلومات شخصية، مثل استخدام تقنيات الإقناع أو الخداع.

عمليات تخمين أو كسر كلمات المرور للوصول إلى البيانات.

التتبع غير المرغوب فيه للأنشطة عبر الانترنت، مما يمكن جمع بيانات شخصية.

عندما يحصل أفراد أو مؤسسات على البيانات الشخصية دون إذن، سواء كان ذلك عن طريق الخطأ أو الإهمال.

عواقب انتهاكات البيانات

التأثير على الأفراد

فقدان الخصوصية

إذا تم الكشف عن بيانات شخصية يمكن استخدامها لأغراض غير مشروعة مثل الاحتيال.

الضرر النفسي

يمكن أن يسبب الانتهاك شعوراً بعدم الأمان والقلق.

التأثير على المؤسسات

فقدان الثقة

ستفقد المؤسسة ثقة جمهورها، مما يعرض سمعتها للخطر.

العقوبات القانونية

قد يعرض المخالفون لعقوبات قانونية شديدة، بما في ذلك غرامات مالية كبيرة.

تكلفة الإصلاح

قد تكون هناك تكاليف عالية لإصلاح الضرر وتعزيز الأمان.

التأثير على الجامعة

التأثير على الأفراد

- انتهاكات البيانات يمكن أن تعرض بيانات الأبحاث القيمة للخطر.
- السمعة الأكاديمية للجامعة قد تتأثر سلباً مما يقلل من جاذبيتها للطلاب والباحثين.

تأمين أجهزتك خط دفاعك الأول

أجهزة الكمبيوتر والهواتف الذكية والأجهزة اللوحية هي بوابات رئيسية للوصول إلى البيانات الشخصية، لذا يعتبر تأمينها أول خط دفاع في حماية البيانات.

التحديث المستمر

حدث النظام والبرامج لغلق الثغرات.

مكافحة الفيروسات

استخدم برنامج معترف به وحدثه دائماً

كلمات المرور

استخدم كلمات مرور قوية ولا تكر مواقع مختلفة.

التحقق الثنائي

فعل هذه الميزة للحصول على طبقة أمان إضافية.

نسخ احتياطي

أنشئ نسخاً احتياطي للبيانات الهامة.

القفل الفيزيائي

استخدامه للحماية من السرقة.

نصائح إضافية

1. تجنب الاتصال بشبكات wifi العامة.
2. لا تقم بتنزيل التطبيقات من مصادر مجهولة.
3. أوقف خاصية Blueuooth عند عدم الحاجة له.

السلوك الأمن على الإنترنت مفتاحك لحماية بيانتك

الإنترنت أداة قوية للتواصل والتعلم، لكنه يحتوي أيضا على مخاطر يجب أن تكون على داريه بها.
السلوك الامن على الإنترنت يعد من الإجراءات الأساسية لحماية البيانات الشخصية

فحص المصدر

قبل النقر على روابط أو تحميل الملفات، تحقق من مصادرها.

الحذر مع المعلومات الشخصية

شاركها فقط مع مواقع معترف بها وآمنه.

تصفح خاص

استخدمه للحد من تتبعك عند بحثك عن معلومات حساسة.

الحذر من التصيد الإلكتروني

لا تنقر على روابط أو تفتح مرفقات من مرسلين مجهولين.

قواعد النشر

كل ما تنشره يستطيع أن يبقى للأبد، فكن حذراً.

المسؤولية الجماعية

حمايتك لنفسك تعني حماية الجميع، لنكن جزءاً من حلول الأمان الرقمي.

إرشادات التعامل مع البيانات الشخصية ومشاركتها

البيانات هي أصل قيم يجب التعامل معه بحذر واحترام. هذه الصفحة تقدم إرشادات حول كيفية التعامل مع البيانات الشخصية وشاركتها بأمان.

أساسيات التعامل مع البيانات

التحقق من البيانات

قبل مشاركة أي بيانات، تأكد من صحتها ودقتها.

النسخ الاحتياطي

يعد النسخ الاحتياطي للبيانات ضرورياً للحفاظ عليها آمنه ومتاحة في حالة حدوث خلل أو فقدان.

التشفير

استخدام التشفير لحماية البيانات الحساسة، خصوصاً عند التخزين أو النقل عبر الشبكات.

أفضل الممارسات لمشاركة البيانات

التحقق من الهوية

قبل مشاركة البيانات، تأكد من هوية الجهة المستقبلة وأنها جديرة بالثقة.

الأذونات

فقط منح الأذونات المناسبة للأفراد الذين يحتاجون الوصول إلى البيانات.

البروتوكولات الأمنة

استخدم بروتوكولات أمنة لنقل البيانات، مثل HTTPS بدلا من HTTP

توقيعات رقمية وشهادات

استخدم التوقيعات الرقمية أو الشهادات للتحقق من أصل البيانات والحفاظ على سلامتها.

العمل من المنزل بأمان

في ظل تزايد الاعتماد على عمل عن بعد، يصبح العمل من المنزل جزءاً لا يتجزأ من ثقافة العمل، ولكن مع هذه الحرية يأتي أيضا المسؤولية في الحفاظ على أمن البيانات.

نصائح للعمل الامن من المنزل

الاتصال الآمن

استخدم VPN (شبكة خاصة افتراضية) لتأمين الاتصال بين جهازك وشبكة العمل.

فحص الأمان

تأكد أن جميع برامج مكافحة الفيروسات وجدران الحماية محدثة.

مكان العمل

خصص مكاناً في المنزل للعمل يكون خالياً من المخاطر المحتملة للأمان البياني.

الحفاظ على الخصوصية

لا تترك جهازك مفتوحاً ومتاحاً للأخرين حتى أفراد العائلة.

التحقق من الهوية

استخدم التحقق الثنائي وأساليب أخرى للتأكد من البيانات الحساسة.

التواصل والتعاون

للتواصل والتعاون استخدم الأدوات المعترف بها التي تفضلها المنظمة والتي تعتبر آمنة.

كن حذراً في المشاركة

عند مشاركة الشاشة أو إرسال ملفات، تأكد من عدم إظهار أو نقل معلومات حساسة.

سياسة حماية البيانات الشخصية للأطفال ومن في حكمهم

الهدف

تهدف هذه السياسة إلى وضع متطلبات حماية البيانات الشخصية للأطفال ومن في حكمهم بجامعة الحدود الشمالية وفق أفضل الممارسات المحلية والدولية، كما تهدف إلى الالتزام بالمتطلبات التشريعية الخاصة بها في وثيقتي ضوابط إدارة البيانات وحوكمتها وحماية البيانات الشخصية (الإصدار: يناير 2021 م)"، و" سياسات حوكمة البيانات الوطنية الإصدار الثاني: مايو 2021 م) الصادرتين عن مكتب إدارة البيانات الوطنية.

النطاق

تطبق هذه السياسة على جهات الجامعة التي تتعامل بشكل مباشر مع البيانات الشخصية للأطفال ومن في حكمهم.

الامتثال لهذه السياسة

يجب على جميع منسوبي الجامعة والمتعاقدين معها الالتزام بهذه السياسة، وعلى جهات الجامعة التي تعمل مع البيانات الشخصية للأطفال ضمان تطبيق هذه السياسة داخل إداراتها، علما بأن الالتزام ببنود هذه السياسة يخضع لمراجعة دورية من مكتب إدارة.

حقوق الأطفال ومن في حكمهم

منح الطفل ومن في حكمه حقوق البيانات عبر وليه وفق سياسة الجامعة.	الحق في طلب إتلاف بياناته بعد بلوغ السن النظامية أو انتهاء الولاية.

القواعد العامة لنقل البيانات الشخصية خارج الحدود الجغرافية للمملكة

الهدف

تهدف هذه السياسة إلى الالتزام بالقواعد العامة لنقل البيانات الشخصية خارج الحدود الجغرافية للمملكة بجامعة الحدود الشمالية وفق أفضل الممارسات المحلية والدولية، والالتزام بالمتطلبات التشريعية الخاصة بها الصادرة عن مكتب إدارة البيانات الوطنية.

النطاق

يجب على منسوبي الجامعة والمتعاقدين الالتزام بالسياسة، خصوصاً فيما يتعلق ببيانات الأطفال، هذا الالتزام يخضع لمراجعة دورية من مكتب إدارة البيانات بالجامعة.

حقوق أصحاب البيانات

إشعار المعني بنقل بياناته خارج المملكة.	الحق في التراجع عن موافقة نقل البيانات.	الحق في الوصول للبيانات المفتوحة.

التزامات الجهات

3. التأكد من اعتماد الجهة المعالجة خارجياً.
1. توفير مستوى كافٍ من الحماية إذا لم تكن الجهة معتمدة.
2. وضع ضمانات لحماية البيانات إذا لم يكن هناك حماية كافية.
4. الحصول على استثناءات عند عدم التوفر لضمانات الأمان.
5. موافقة مكتب إدارة البيانات بالجامعة قبل النقل.

أدوات الحماية

البرمجيات الأمنية

مكافحة الفيروسات

تعتبر برامج مكافحة الفيروسات الحائط الأول في خط الدفاع ضد التهديدات الأمنية.

الجدار الناري (Firewall)

يستخدم لمنع الوصول غير المصرح به إلى الشبكات والأنظمة

أدوات التشفير

استخدامها لتأمين البيانات عند الحفظ والنقل.

التطبيقات المحمولة

تطبيقات الأمان

استخدم تطبيقات موثوقة لحماية البيانات على الأجهزة المحمولة.

تطبيقات مراقبة الشبكة

تستخدم لرصد نشاط الشبكة والتأكد من عدم وجود نقاط ضعف.

إرشادات مشاركة البيانات الشخصية في المواقع والتطبيقات

تأكد من معرفة كيف يتم التعامل مع بيانتك قبل مشاركتها في المواقع الإلكترونية والتطبيقات:

مواقــع الانترنت

1 **إشعـــار الخصوصيـــة**
توضـح كيفيـة جمع البيـانـات واستخدامهـا.

2 **الاطـلاع على الأحكـام**
يـحـدد الـقـواعـد والمسـؤوليـات بينك وبين الموقع.

3 **الأسئلـة الشائعـة**
توفر إجابات لأكثر الاسـتفسـارات شيـوعـاً.

4 **الشهـادات الأمنيـة**
تأكد من أن الصفحة تبدأ بـHttps للتحقق من الأمـان.

5 **التقييمـات والمراجعات**
قم ببحث سريع لمعرفة تجارب الآخريـن.

التطبيقات الإلكترونية

1 **سيـاسـة الخصوصيـة**
توضح كيف يتم جمـع ومـعـالـجـة وحفـظ بيانـاتـك.

2 **التحـقق مـن الصلاحيـات**
مراجعة الصلاحيات التـي يـطـلـبـهـا التطبيق والتـأكـد مـن أنـهـا مـبـررة لوظيفة التطبيـق.

3 **تحـديـث التطبيقـات**
تحديث التطبيقات بـانتظـام لتـأكيـد تـفـعـيـل أحـدث الإجـراءات الأمنيـة.

4 **التحـقق الثنـائـي**
إذا كـان التطبيق يوفر خاصيـة التحقق الثنائي فهي تعزز من أمان الحسـاب.

5 **التقييمـات والمراجعات**
قم بقراءتها لفحص مدى الأمـان والجـودة للتطبيـق.

التعلم المستمر

حماية البيانات عملية مستمرة تتطلب التعلم والتطوير المستمر. سنقدم مصادر التعلم لضمان حماية البيانات بفعالية.