سياسات تداول المعلومات

سياسات الاستخدام والنشر على البوابة الإلكترونية

تراجع هذه الوثيقة سنوياً بتحديثها عن طريق جامعة القصيم فقط؛ لاحتمال وقوع مؤثرات داخلية أو خارجية عليها قد تؤثر على صحتها. ويحتفظ بنسخة موقعة من هذه الوثيقة في مخزن وثائق جامعة القصيم –عمادة تقنية المعلومات - سياسات.

- تسعى جامعة القصيم لتحقيق العديد من الأهداف، من خلال البوابة الإلكترونية للجامعة تتمثل في الآتي:
- التركيز على نقل قيم الجامعة ورؤيتها ورسالتها.
- تعزيز مجموعة واسعة من الفرص الوظيفية المتاحة في جامعة القصيم.
- تشجيع مستخدمي موقع الجامعة لزيارة الحرم الجامعي، وحضور الفاعليات بالجامعة، وطلب المعلومات.
- توفير معلومات دقيقة ومتسقة عن إنجازات جامعة القصيم.
- تأكيد توطيد العلاقات الأكاديمية بين أعضاء هيئة التدريس والطلاب.
- تسليط الضوء على فرص الدراسة والبرامج المتميزة التي تقدمها جامعة القصيم.
- تجنب لوحات الإعلانات الخاصة للإدارات والكليات.
- الوصول للخدمات الإلكترونية المقدمة لمنسوبي الجامعة بشكل سهل وميسر.

الهدف:

تهدف هذه السياسات إلى وضع ضوابط الاستخدام والنشر للبوابة الالكترونية، وكيفية إدارة المحتوى بمواقع البوابة الالكترونية وفقاً لمضمون جملة السياسات المخصصة لضبط التعاملات الإلكترونية بجامعة القصيم.

نطاق التطبيق:

تطبق هذه السياسات على جميع مستخدمي البوابة الإلكترونية للجامعة وكذلك المسئولين عن النشر وإدارة المحتوى بالمواقع التابعة للبوابة الإلكترونية بجامعة القصيم.

مفاهيم البوابة الإلكترونية

- البوابة هي الموقع الإلكتروني لجامعة القصيم وكل ما يتبع له من مواقع نشر المحتوى سواء أكان موقع كلية أم عمادة أم إدارة أم موقعاً خاصاً بعضو هيئة تدريس أو موظف أو طالب.
- شروط الاستخدام هي جميع الشروط والضوابط التي يجب أن تراعى عند استخدام البوابة الإلكترونية بجامعة القصيم.

- المحتوى هو النصوص أو الرسوم البيانية أو الإعلانات أو الروابط أو غيرها من المواد كأخبار الجامعة، وفعاليات الجامعة، والمرئيات، وبيانات التواصل بمنسوبي الجامعة، والمقررات الدراسية والمقالات المنشورة.

- الروابط الخارجية هي الروابط التي تنقل التصفح إلى صفحات لا تتبع لبوابة جامعة القصيم.

شروط الاستخدام

- تعد البوابة الموقع الرسمي الوحيد لجامعة القصيم وتدار من قبل عمادة تقنية المعلومات ممثلة بقسم البرمجيات وإدارة البوابة الالكترونية، ويدار المحتوى فيها من خلال العمادات، والكليات، والإدارات ومراكز الجامعة وكلا بما يعبر عن نفسه.

- على جامعة القصيم إتاحة شروط الاستخدام للبوابة الالكترونية على جميع صفحات البوابة.

- يجب على المستخدم معرفة أن استخدامه لبوابة جامعة القصيم يعد قبولاً منه بشروط استخدام البوابة ، فإذا كان لا يقبلها بالكامل فإن دخوله لهذا الموقع أو أي موقع فرعي يعد تعدياً وعليه أن يتوقف عن استخدامه فوراً.

حجز النطاقات الفرعية

- يجب أن تكون استضافة مواقع جامعة القصيم على الشبكة العالمية من خلال الجامعة، أو من خلال جهات حكومية أخرى، أو من خلال مقدمي خدمات الاستضافة الذين رخصت لهم هيئة الاتصالات وتقنية المعلومات. على أن تكون الاستضافة داخل المملكة، وأن يتضمن العقد المبرم بين الطرفين ضوابط لضمان سرية المعلومات.

- يحق لكل جهة بالجامعة حجز نطاق أو اسم مختصر ليكون تابع لمجال الجامعة (qu.edu.sa) وذلك بتقديم خطاب رسمي إلى (عمادة تقنية المعلومات) موضح فيه الاسم المختصر المطلوب حجزه.

- لا يحق لأي جهة بجامعة القصيم إنشاء موقع إلكتروني تابع لها خارج المجال (qu.edu.sa).

صلاحية إدخال المحتوى وتحديثه

- تقع مسئولية الاضافة أو الحذف أو التعديل على علامات التبويب بالصحفة الرئيسية لبوابة الجامعة على عاتق قسم البرمجيات والبوابة الالكترونية التابعة لعمادة تقنية المعلومات بجامعة القصيم أو من تنيبها.

- تقع مسئولية إدارة صحيفة الجامعة الإلكترونية على مركز الاعلام والاتصال بالجامعة حيث إن لديه كامل الصلاحية في نشر وتحديث محتويات الصحيفة الإلكترونية وكذلك كل ما هو متعلق بالأخبار والفعاليات والندوات والمؤتمرات والمقالات وما يندرج تحتها من خدمات خاصة بها.

- على اي جهة من جهات جامعة القصيم ترغب بنشر اخبار أو فعاليات أو ندوات أو مقالات أو مؤتمرات على الصفحة الرئيسية لبوابة الجامعة التواصل مع مركز الاعلام والاتصال بالجامعة بشكل رسمي .

- في حال وجود إضافة برمجية (كإضافة نموذج تسجيل حضور على سبيل المثال ولا الحصر)، يجب أن يتم تزويد قسم البرمجيات والبوابة الالكترونية بعمادة تقنية المعلومات بخطاب رسمي عبر وسائل الاتصالات الإدارية يحتوى على الطلبات بمدة لا تقل عن ثلاث أسابيع قبل تاريخ انعقاد المؤتمر أو الفعالية ، وبغير ذلك

لن يتم النظر الي الطلب .

- كل جهة من جهات الجامعة لديها موقع مستقل بصلاحية إدارته بشكل كامل، بحيث تقع مسئولية نشر وتحديث المحتوى الإلكتروني الخاص بكل جهة على عميد أو مدير الجهة المسؤول ويتحمل مسئولية نشر وتحديث كامل محتوياته، كما أن لكل عضو هيئة تدريس أو موظف أو طالب أو طالبة موقع مستقل.

- لا تلتزم عمادة تقنية المعلومات بمراجعة الروابط الخارجية المتصلة بالبوابة، ولا تتحمل العمادة مسؤولية المحتوى أو الخدمات التي تقدمها المواقع المسجلة خارج نطاق البوابة الرسمية للجامعة.

النشر على البوابة

- تعد البوابة وسيلة نشر إلكتروني لجميع منسوبي الجامعة وقطاعاتها وعليهم استخدامها فيما يعود بالنفع على الجامعة ومنسوبيها وقطاعاتها المختلفة وبما لا يخل بأي شكل من الأشكال بسمعة الجامعة ومنسوبيها أو يعرضهم للمساءلة القانونية.

- كل المحتوى المنشور في صفحات البوابة يجب أن يتوافق مع حقوق النشر، وعليه يمنع نشر الآتي دون الحصر:

- أي مواد إلكترونية غير مملوكة لصاحب الصفحة ولها حقوق نشر

- البحوث المنشورة في مؤتمرات علمية ومجلات علمية.

- الكتب والمؤلفات المتوفرة بأي صيغ إلكترونية.

- المحتوى غير الملائم ويشمل الآتي دون الحصر:

- ما يحتوي على لهجة نابية أو متهجمة أو عنصرية أو مهددة سواء أكان نصاً أم صورة أو فكرة.

- ما يخالف أنظمة الدولة والجامعة أو أعراف المجتمع.

- ما يتعرض لخصوصية الآخرين بأي شكل من الأشكال.

- على كل جهة بالجامعة لها موقع تابع لبوابة الجامعة التأكد من تحديث محتوى الصفحات والمواد بما في ذلك الأخبار ومعلومات الاتصال وأرقام الهواتف والبريد الإلكتروني ووصف المواد وغيرها من المعلومات.

- على الجميع استخدام قواعد اللغة المستخدمة لإنشاء الصفحة أو المادة الإلكترونية والتأكد من سلامتها وخلوها من الأخطاء.

- تحتفظ عمادة تقنية المعلومات بالحق في التغيير او الحذف للمعلومات الواردة في أي موقع تحت مظلة الجامعة في أي وقت دون سابق إنذار في حال الاخلال بسياسات البوابة للنشر وإدارة المحتوى.

الخصوصية

- على عمادة تقنية المعلومات بجامعة القصيم إتاحة سياسة الخصوصية على جميع صفحات البوابة، توضيحًا لحقوق وواجبات موقع الجامعة والمواقع التابعة لها ومستخدميها، وعليه تلتزم جامعة القصيم بحماية سرية وخصوصية المستخدم.
- تحتوي سياسات الخصوصية على كيفية تعامل جامعة القصيم مع معلومات المستخدم الشخصية فيما يتعلق بالبيانات سواء أكانت على الإنترنت أم على أجهزة الكمبيوتر فقط.
- تتصل بعض الروابط على موقع جامعة القصيم بمواقع أخرى غير تابعة للجامعة (ليست ضمن المجال qu.edu.sa) وهذه المواقع لا تعمل وفقًا لسياسة الخصوصية المتبعة في موقع جامعة القصيم لذا على الزائر مراجعة سياسة الخصوصية الخاصة بتلك المواقع قبل الكشف عن أي معلومات شخصية تدل على صاحبها.

الإشراف والتدريب

- يحق لكل جهة بالجامعة أن تخصص مشرفاً أو أكثر خاصاً بها، حيث يعطى هذا المشرف الصلاحيات اللازمة على حسابه الجامعي المستخدم في نظام الدخول ويكون بذلك المسئول عن الموقع الإلكتروني للجهة ومحتواه وجميع المهام اللازمة لضمان استمرارية العمل بالموقع.
- تلتزم عمادة تقنية المعلومات بتقديم التدريب اللازم لإدارة الموقع الإلكتروني (لأي جهة لديها موقع إلكتروني تحت مظلة البوابة)، حيث يتم التنسيق لذلك أو طلبه من خلال خطاب رسمي لعمادة تقنية المعلومات.
- يحق لكل عضو هيئة تدريس ومن في حكمه في الجامعة الحصول على التدريب اللازم لإدارة صفحته الشخصية تحت صفحات أعضاء هيئة التدريس.
- يحق لأعضاء هيئة التدريس ومن في حكمهم الحصول على التدريب اللازم لإدارة صفحاتهم الشخصية ضمن صفحات أعضاء هيئة التدريس أو مواقع الجهات وذلك بالتنسيق مع عمادة تقنية المعلومات بشكل مباشر.

السياسات المتعلقة بالشبكة الداخلية

- لا يسمح باستخدام اتصال VPN إلا عند الضرورة وللأشخاص المحددين وفقاً للتالي:
  - الشخص الذي لديه صلاحية تقديم الدعم التقني الطارئ على أحد الأنظمة الإلكترونية للجامعة.
  - مدير النظام الذي يحدده مالك الخدمة (business owner).
  - الموردين المعتمدين من عمادة تقنية المعلومات بعد التوريدات والتركيبات اللازمة.
- يتم طلب الخدمة وفقاً لمخطط سير العمل المحدد مسبقاً والمعتمد من عميد عمادة تقنية المعلومات.

- على عمادة تقنية المعلومات تشفير الحساب الشخصي المعتمد والمستخدم للاتصال بشبكة الجامعة من خلال خدمة SSL VPN أثناء العبور عبر شبكات غير مؤمنة وموثوق بها.
- يجب استيفاء متطلبات التعقيد والصعوبة الخاصة بكلمات المرور وفقاً لسياسة (user password management)
- يجب على الموظفين المصرح لهم من قبل الجامعة التأكد من ألا يتم السماح للمستخدمين الغير مصرح لهم بمشاركة خدمات الـ VPN الخاصة بالجامعة، أو الحصول على كلمة المرور الخاصة بهم، أو الوصول واستخدام جهاز الكمبيوتر أثناء عملية الاتصال.
- تأمن جميع أجهزة الكمبيوتر المتصلة بشبكة الجامعة من خلال خدمة الـ VPN وفقاً لمعايير عمادة تقنية المعلومات الخاصة بالبرامج المضادة للفيروسات بأحدث إصدارات للملفات الخاصة بها وكذلك آخر تحديث من تصحيحات الأمان الخاصة بنظام التشغيل.
- يمكن فقط استخدام تطبيقات الاتصال الخاصة بالكمبيوتر المعتمدة لفتح قنوات اتصال بشبكة الجامعة من خلال خدمة ال .VPN
- سيتم قطع الاتصال تلقائياً عن الموظفين المصرح لهم بالدخول على شبكة الجامعة من خلال خدمة الـ VPN بعد ساعة واحدة من عدم النشاط.
- تخضع أجهزة الكمبيوتر للموظفين المصرح لهم بالدخول على الشبكة من خلال خدمة الـ VPN وفقاً لاحتياجات العمل الخاصة بهم لتقييد الوصول إلى الشبكة.
- على عمادة تقنية المعلومات فحص ورصد ومراجعة جميع قنوات اتصال الـ VPN بجامعة القصيم.
- يمنع منح اتصال VPN إذا كان المستفيد خارج المملكة العربية السعودية إلا في حالات الضرورة، ولعمادة تقنية المعلومات الحق في الرفض أو السماح.
- لعمادة تقنية المعلومات الحق في المراقبة أو التحديد أو الفصل لأي اتصال VPN ولأي غرض دون إشعار مسبق.

سياسة كلمة المرور (Password Policy)

- عندما يتم إنهاء علاقة موظف أو عميل أو شريك لديه صلاحية الوصول إلى أصول (بيانات او معلومات) جامعة القصيم (بشكل مؤقت أو نهائي)، يجب إلغاء جميع الصلاحيات فورا.
- يجب تغيير كلمة المرور التلقائية عند تفعيل حساب جديد، قبل دخولها إلى بنية جامعة القصيم التحتية وقبل وضعها في بيئة العمل.
- خلال عملية الدخول إلى انظمة المعلومات الخاصة بجامعة القصيم، كلمة المرور يجب أن لا تظهر على الشاشة. يجب على المستخدم التأكد من أنه غير مراقب وحقل دخول كلمة المرور يعرض رموز (رمز النجمة مثلا) لكل حرف يتم كتابته (إخفاء كلمة المرور).
- إقفال اسم المستخدم وانتهاء صلاحية كلمة المرور يجب تعريفها بناء على تصنيف الأصول ومتطلبات الأمان.
- يجب على المستخدمين ذوي الامتيازات والمستخدمين العاديين استخدام كلمات مرور مختلفة لكل حساب يملكون صلاحية الوصول إليه. في حالة البنية التحتية لإدارة المستخدمين المركزية. وفي حال الدخول الموحد يجب أن يتم تطبيق التحقق الثنائي للوصول.
- يجب على المستخدم والمدير إتباع شروط الأمان التالية عند اختيار كلمة المرور:
  - يجب ان تكون ثمانية حروف على الأقل.
  - يجب أن تشمل حروف (أحرف كبيرة وأحرف صغيرة) وأرقام ورموز.
  - كلمة المرور يجب ألا تشمل كامل أسم المستخدم.
  - عدم تفعيل خيار تذكر كلمة المرور.

- يجب أن يغلق الحساب لمدة ١٥ دقيقة بعد خمس محاولات دخول خاطئة.
- على كل مدير نظام من أنظمة المعلومات بجامعة القصيم تغيير كلمة المرور الخاصة به عل الأقل كل ١٢٠ يوما.
- على كل مستخدم من مستخدمي أنظمة المعلومات تغيير كلمة المرور الخاصة به عل الأقل كل ١٨٠ يوما.
- يجب عدم تخزين كلمة المرور على الأنظمة أو يتم نقلها عبر الشبكات الداخلية أو الخارجية بدون أن تكون مشفرة.
- كلمات مرور جميع الأصول التي تتطلب تسجيل الدخول يجب تغييرها فورا في حال الاشتباه أو التأكد أن كلمة المرور تم الإفصاح عنها لدى مستخدمين غير مصرح لهم.

استخدام كلمة المرور

- يجب على مستخدمي المعلومات إتباع سياسات أمان جامعة القصيم في اختيار واستخدام كلمة المرور بناء على سياسة إدارة كلمة مرور المستخدم.
- يجب على مستخدمي المعلومات عدم مشاركة حساباتهم وكلمات المرور الخاصة فيهم مع الآخرين حيث أنهم مسؤولون عن أي نشاطات تصدر من حساباتهم.
- يجب على جامعة القصيم أن تتبنى نظام تفاعلي لإدارة كلمة المرور للتأكد من كفاءة كلمة المرور وتوافقها مع سياسة إدارة كلمة مرور المستخدم.

سياسة النسخ الاحتياطي (Backup Policy)

- يجب على عمادة إدارة تقنية المعلومات بالتعاون والترتيب مع مالكي الانظمة وضع خطة نسخ احتياطي واستعادة لجميع أصول (البيانات والمعلومات) جامعة القصيم مع الأخذ بالاعتبار التالي:
  - المتطلبات القانونية والتنظيمية.
  - تصنيف الأصول (البيانات والمعلومات).
  - توصيات الموردين.

- يجب على خطة النسخ الاحتياطي والاستعادة أن تحدد التالي:
  - نوع النسخ الاحتياطي.
  - جدول النسخ الاحتياطي.
  - حماية النسخ الاحتياطي (بناء على تصنيف البيانات المنسوخة).
  - الاحتفاظ بالنسخ الاحتياطي.

- يجب أن يتم مراجعة واختبار البيانات المنسوخة احتياطيا بشكل دوري. (كل ثلاثة أشهر) للتأكد سلامتها وفعاليتها خلال عملية استعادة بيانات محددة
- عملية استعادة النسخ الاحتياطية يجب أن تتطلب التفويض المناسب من مالك النظام ويجب تنفيذها وفقا لعملية النسخ الاحتياطي وعملية استعادة البيانات.
- يجب استبدال وسائط النسخ الاحتياطي فورا في حال مواجهة عطل أو على فترات زمنية محددة مسبقا أيا كان الأسبق.

- يجب تسمية وسائط النسخ الاحتياطي بشكل مناسب وترقيمها بشكل تلقائي عن طريق نظام النسخ الاحتياطي متى ما أمكن أو يدويا من قبل مدير النظام المسؤول عن النسخ الاحتياطي.
- يجب أن تحتوي وسائط النسخ الاحتياطي على معايير التحديد التالية والتي يمكن التعرف عليها بسهولة بواسطة نظام التسمية:
  - اسم النظام.
  - تاريخ الإنشاء.
  - التصنيف.
  - فترة الحفظ.
- تخزين النسخ الاحتياطي:
  - داخل الموقع: البيانات المنسوخة داخل الموقع يجب أن يتم الحفاظ عليها في حصانة آمنة، يفضل أن تكون خارج غرفة النظام وداخل خزانة آمنة.
  - خارج الموقع: البيانات المنسوخة خارج الموقع يجب الحفاظ عليها في موقع خارجي متى ما أمكن.
- سجلات النسخ الاحتياطي يجب أن تراجع من قبل مدير النظام المختص للتأكد من صحة النسخ.
- سجلات النسخ الاحتياطي يجب أن يتم مراجعتها وتحديثها دوريا.
- يجب أن تكون النسخ الاحتياطية التي تحتوي على بيانات مصنفة على أنها "سري" أو أعلى مشفرة متى ما أمكن.

سياسة إدارة واستخدام الأنظمة Systems Use Policy

- على جميع الأنظمة في جامعة القصيم إتباع سياسة الاستخدام المقبول لأنظمة المعلومات.
- أي تغيير يطرأ على الأنظمة يجب عليه إتباع إجراء إدارة التغيير.
- على جميع الأنظمة في جامعة القصيم إتباع سياسة النسخ الاحتياطي.
- على مالك النظام أن يكون مسؤول عن تحديد ما يلي، لكن غير محصور عليه:
  - مجموعات دخول المستخدم.
  - حقوق دخول للمستخدم.
- طلب سجل الدخول يجب أن يكون مصدق عليه من مالك النظام ومدير قسم الطلبات قبل تعيين الصلاحيات لمستخدمي المعلومات.

- يجب توفير تسجيل الدخول إلى النظام لمستخدمي المعلومات لتأدية أنشطتهم المتعلقة بالعمل، بالإضافة إلى أنه يجب توفير تسجيل الدخول على أساس الحاجة إلى المعرفة قاعدة الصلاحيات الأقل.
- يجب تسجيل صلاحيات الدخول في قائمة خاصة بالتحكم بتسجيل الدخول. هذا النوع من السجلات يجب
- يجب تجنب معرفات المستخدمين التي قد توضح مستوى صلاحية المستخدم (مسؤول مثلا).
- يجب التحكم بصلاحية الدخول إلى أنظمة جامعة القصيم بواسطة آليات أمان مناسبة بناء على التالي:
  - مستوى الثقة (موثوق وشبه موثوق وغير موثوق).
  - مستوى الدخول (بسيط أو دخول ذو صلاحيات).
  - نوع الدخول (داخلي أو عن بعد أو الدخول إلى أنظمة طرف ثالث).
- يجب مراجعة دخول المستخدم وصلاحياته سنويا على الأقل بواسطة مالك النظام بالتعاون مع عمادة تقنية المعلومات.
- يجب أن تكون مراجعة دخول المستخدمين وصلاحياتهم مرتبط بالتغيرات التي تطرأ على النظام المستخدم وتغير في الموقع ومتطلبات الامتثال التنظيمي.
- يجب على جامعة القصيم إدارة الأحداث التالية ووضع بنود لتحليل الخبراء للبيانات لإيجاد الاختلافات أو الثغرات المحتملة أو الحوادث الأمنية:
- يجب على مدير إدارة النظام مراقبة التالي:
  - سجلات الدخول والخروج الناجحة والفاشلة.
  - إعادة تشغيل وإيقاف تشغيل النظام الناجح والفاشل.
  - تغيرات سياسات الأمان الناجحة والفاشلة.
  - إدارة المستخدم والمجموعة الناجحة والفاشلة.
  - الدخول إلى الملفات الناجح والفاشل.
  - استخدام حقوق المستخدم الناجح والفاشل.
- يجب على عمادة تقنية المعلومات مراقبة التالي:
  - نتائج أنماط الاستخدام "الطبيعي" مثل:
  - حمل النظام في أوقات مختلفة من اليوم.
  - عدد العمليات قيد التشغيل.
  - استخدام وحدة المعالجة المركزية.
  - نجاحات غير عادية رفض الاتصالات.
  - نجاحات ورسائل الأخطاء الخاصة بالجدران النارية.

- محاولات الدخول المتكررة.
- الدخول لمنافذ غير اعتيادية.

- على جامعة القصيم التأكد أن ضوابط أمن المعلومات المطبقة مفعلة ولا يتم تجنبها. يجب أن تشمل المراقبة النشاطات التالية ولكن غير محصورة عليها:
  - سجلات كشف التسلل إلى النظام.
  - سجلات الجدار الناري.
  - سجلات حساب المستخدم.
  - سجلات مسح الشبكة.
  - سجلات أمان التطبيق.
  - سجلات الأمان.
- يجب على جامعة القصيم مراجعة نتائج مراقبة النشاطات بناء على المخاطر المحتملة. يجب وضع بعين الاعتبار عوامل الخطر التالية (لكن غير محصور عليها):
  - نسبة اهمية الاصول المعنية.
  - تجربة مسبقة لاختراق أو سوء استخدام النظام بالإضافة إلى التكرار في استغلال الثغرات.
  - مدى ترابط النظام (خاصة الشبكات العامة).
  - إلغاء تنشيط منشأة التسجيل.

- يجب على جامعة القصيم ضمان صلاحية ونزاهة البيانات المدخلة إلى التطبيقات عن طريق:
  - تحديد الحقول لتسمح بنطاق معين من البيانات (تحديد القيم خارج النطاق أو تحديد نطاق قيم البيانات العليا أو السفلى).
  - التحقق من وجود حروف غير صالحة في حقل البيانات.
  - وضع الحقول المهمة إلزامية.
  - التحقق من قابلية البيانات المدخلة بالاعتماد على قوانين العمل.
  - الحماية ضد الهجمات الشائعة (تجاوز سعة المخزن المؤقت وهجمات الحرمان من الخدمات).
  - استخدام أرصدة التحكم للتأكد من استكمال المدخلات والمعالجة.

- يجب أن يتم التحقق من نتائج معالجة البيانات للتأكد من صحتها. يجب تطبيق التالي:
  - التحقق من النتائج لتحديد القيم الغير صالحة لمنع الهجمات مثل هجوم حقن الشيفرة المصدرية.
  - التحقق من تصنيف النتائج للتأكد من تعيين التصنيف الصحيح (يجب ألا يمكن الدخول إلى البيانات السرية بواسطة مستخدم غير موثوق).
- يجب وضع إجراءات معالجة الاخطاء لتجنب عرض تفاصيل رسالة الخطأ للمستخدمين.

QU Saudi Arabia

Qassim University جامعة القصيم

رؤية VISION 2030

المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

سياسات تداول المعلومات

www.qu.edu.sa