عمادة تقنية المعلومات
والتعليم الإلكتروني
Deanship of Information
Technology & E-Learning

معتمد
ACCREDITED

جامعة حائل
University of Ha'il

رؤية VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

سياسة اقتناء الأنظمة وتطويرها وصيانتها

بجامعة حائل

2023/2022م


بسم الله الرحمن الرحيم

سياسة اقتناء الأنظمة وتطويرها وصيانتها بجامعة حائل

عمادة تقنية المعلومات
و التعليم الإلكتروني

Deanship of Information
Technology & E-Learning

معلومات ذات ملكية فكرية:

الرقابة على الوثيقة

معلومات عن الوثيقة

العنوان	التصنيف	الإصدار	الحالة
سياسة اقتناء الأنظمة وتطويرها وصيانتها	عام	2.0	معتمدة

الإعداد والتحديث

الإصدار	المؤلف / المؤلفون	تاريخ الإصدار	التغييرات
0.1			إعداد
0.2			مراجعة
0.3			تحديث
1.0			مسودة
1.1			
1.2			
2.0			

قائمة التوزيع

#	المستفيد
1	إدارة الشؤون القانونية
2	الموقع الالكتروني للجامعة
3	قسم ضمان الجودة بالعمادة
4	قسم إدارة الأنظمة بالعمادة
5	قسم الشؤون الإدارية والمالية بالعمادة

الاعـــــتماد

الاسم	الصفة	التاريخ	التوقيع
د. خالد بن عبدالعزيز العتيبي	عميد تقنية المعلومات والتعليم الإلكتروني		

نظرة عامة على السياسة:

يستعرض هذا الجزء بالتفصيل الغرض من هذه السياسة ونطاقها وتعريف مصطلحاتها، وتغييرها، ومراجعتها وتحديثها، وإنفاذها/والامتثال لها، والأدوار والمسؤوليات، والوثائق ذات الصلة بالإضافة ملكية الوثيقة.

الغـــرض:

الغرض الرئيسي من سياسة إدارة المخاطر هو:

التأكد من أن أمن المعلومات هو جزء لا يتجزأ من أنظمة المعلومات عبر دورة الحياة بأكملها، والتأكد من تصميم أمن المعلومات وتنفيذه خلال دورة حياة تطوير نظم المعلومات، وضمان حماية البيانات المستخدمة للاختبار..

النطـــاق:

تنطبق بيانات السياسة المكتوبة في هذه الوثيقة على جميع موارد جامعة حائل على جميع مستويات الحساسية، بما فيها:

- جميع الموظفين بدوام كامل وبدوام جزئي والموظفين المؤقتين الذين يعملون لدى الجامعة، أو يعملون لصالحها أو بالنيابة عنها.
- الطلاب الذين يدرسون في جامعة حائل.
- المقاولون والاستشاريون الذين يعملون لصالح جامعة حائل أو نيابة عنها.
- جميع الأفراد والجماعات الأخرى الذين تم منحهم إمكانية الوصول إلى أنظمة تقنية المعلومات والتعليم الإلكتروني في جامعة حائل.

تغطي هذه السياسة جميع أصول المعلومات المحددة في وثيقة نطاق تقييم المخاطر وسيتم استخدامها كأساس الإدارة أمن المعلومات.

المصطلحات والتعريفات:

- **يوفر الجدول تعريفات للمصطلحات الشائعة المستخدمة في هذه الوثيقة.**

المصطلح	التعريف
المساءلة	مبدأ أمني يشير إلى ضرورة القدرة على تحديد هوية الأفراد وتحميلهم مسؤولية أفعالهم.
الأصول	المعلومات التي تعتبر ذات قيمة بالنسبة للمؤسسة مثل النماذج والوسائط والشبكات والأجهزة والبرامج ونظام المعلومات.
توفر	الحالة التي يكون فيها الأصل أو الخدمة قابلة لأن تصلها جهة مصرح لها بذلك وقابلة لأن تستخدمها أيضا.
السرية	عدم توفير الأصل أو الخدمة أو عدم كشف أي منهما الأفراد غير مصرح لهم أو جهات أو عمليات غير مصرح بها.
الرقابة	وسيلة لإدارة المخاطر تشمل السياسات والإجراءات والإرشادات التي قد تكون ذات طبيعة إدارية عليا أو تقنية أو إدارية أو قانونية.
التشفير	نظام يشتمل على مبادئ ووسائل وأساليب لتحويل البيانات بغرض إخفاء مضمون معلوماتها أو منع تعديلها بطريقة لا يمكن اكتشافها أو منع استخدامها بطريقة غير مصرح بها.
الإرشاد	وصف يوضح ما يجب عمله لتحقيق الأهداف المحددة في السياسات والطريقة التي تحقق بها تلك الأهداف.
توقيع الكتروني	محاولة محاكاة لفعل غير الكتروني لشخص ما وهو يضع توقيعه على ورقة. وتشمل هذه المحاولة تطبيق خوارزمية رياضية بعينها يتم تخزينها عادة على المفتاح الخاص للمستخدم وكجزء منه- على محتويات نص.
أمن المعلومات	الحفاظ على سرية المعلومات وسلامتها وتوفرها. وهو يشمل وسائل أخرى مثل التحقق والمساءلة وعدم التنصل والموثوقية.
السلامة	الحفاظ على الأصول والتأكد من دقتها وتناسقها طوال دورة حياتها بأكملها.
المالك	أي شخص أو مجموعة من الأشخاص تحددهم الإدارة لتحمل مسؤولية الحفاظ على سرية الأصول وتوافرها وسلامتها. وقد يتغير المالك أثناء دورة حياة الأصل.
اختبار الاختراقات	طريقة لتقييم أمن نظام الحاسب الآلي أو الشبكة عن طريق محاكاة هجوم تنفذه جهات خارجية شريرة (ليس لديها وسائل معتمدة للوصول إلى أنظمة الجامعة) وجهات داخلية خبيثة (تتمتع بمستوى معين من الوصول المصرح به). تشمل هذه العملية تحليلا نشطا للنظام للتأكد من خلوه من أي ثغرة أمنية محتملة يمكن أن تنجم عن ضبطه بطريقة سيئة أو غير مناسبة، ووجود عيوب معروفة أو غير معروفة في الأجهزة أو البرمجيات، ووجود ضعف تشغيلي في العملية أو الإجراءات التقنية المضادة. يتم تنفيذ هذا التحليل من موقع مهاجم محتمل ويمكن أن يتضمن استغلالا نشطا لثغرات أمنية.
السياسة	خطة عمل يسترشد بها عند اتخاذ القرارات والإجراءات. وتشمل السياسة تحديد البدائل المختلفة مثل البرامج أو أولويات الإنفاق، والاختيار بينها على أساس التأثير الذي ستحدثه.
الخصوصية	حق الفرد في أن يكون آمنا من الإفصاح غير المصرح به عن معلوماته الشخصية المضمنة في المستندات.
الخطر	مزيج من عواقب الحدث واحتمالات حدوثها (بما في ذلك التغيرات في الظروف).
النظام	جهاز أو نظام مترابط أو أنظمة فرعية من المعدات تستخدم في الحصول على البيانات أو تخزينها أو معالجتها أو إدارتها أو التحكم فيها أو عرضها أو تبديلها أو تبادلها أو نقلها أو استقبالها، بما في ذلك برامج الحاسب الآلي والبرامج الثابتة والأجهزة.
المورد	الطرف الذي يوفر الأجهزة أو الخدمات.
التهديد	الطرف الذي يوفر الأجهزة أو الخدمات. احتمال التسبب في حادثة غير مرغوب فيها قد تؤدي إلى إلحاق الضرر بنظام مثل الكشف غير المصرح به عن المعلومات الحساسة أو الأصول أو الخدمات أو إتلافها أو إزالتها أو تعديلها أو قطعها أو إصابة الأشخاص. وقد يكون التهديد متعمدا أو عرضيا كما قد يكون من مصدر طبيعي.
نقطة الضعف	ضعف الإجراءات أو العمليات أو الضوابط الأمنية التي يمكن استغلالها عن طريق التهديد بالوصول غير المصرح به إلى المعلومات أو تعطيل المعالجة الحرجة.

التغيير، المراجعة والتحديث:

يجب مراجعة هذه السياسة مرة واحدة كل عام ما لم يعتبر المالك إجراء مراجعة سابقة ضرورية لضمان استمرار السياسة الحالية. ولا يجري تغييرات في هذه السياسة إلا ضابط أمن المعلومات على أن تعتمد الإدارة هذه التغييرات. ويجب أن يظل سجل التغيير محدثاً بحيث يخضع للتحديث بمجرد إجراء أي تغيير في السياسة.

الإنفاذ والامتثال:

يعد الالتزام بهذه السياسة أمرة إلزاميا وعلى ضابط أمن المعلومات أن يراجعها بشكل دوري، ويجب على جميع وحدات جامعة حائل (من عمادات، وإدارات، وكليات، وأقسام ومراكز) التأكد من الامتثال لها باستمرار.

في حالة تجاهل أو انتهاك توجيهات أمن المعلومات، قد تتضرر بيئة جامعة حائل (على سبيل المثال، يحدث فقدان للثقة في الجامعة وسمعتها، أو تتعطل عملياتها أو تحدث بها انتهاكات قانونية)، ويكون الأشخاص الذين تجاهلوا هذه التوجيهات أو انتهكوها مسؤولين عما وقعوا فيه من فعل أو ترك مما يؤدي إلى اتخاذ إجراءات تأديبية أو تصحيحية بحقهم (مثل الفصل من الخدمة) ويمكن أن يخضعوا لتحقيقات قانونية.

يجب ضمان معاملة الموظفين الذين يشتبه في انتهاكهم للأوامر الأمنية بطريقة صحيحة وعادلة (مثل الإجراءات التأديبية)، ويجب إبلاغ إدارة الموارد البشرية لمعالجة انتهاكات السياسة عند التعامل مع هذه الانتهاكات.

الاستثناءات:

يجب أن ينظر أمن المعلومات في الاستثناءات على أساس فردي. كما يجب أن يرفق مع طلب الاستثناء حالة العمل المنطقية التي استدعت تقديمه وطلب الموافقة عليه. والجهة المخول لها الموافقة على هذا الطلب هي ضابط أمن المعلومات على أن تعتمد هذه الموافقة عمادة تقنية المعلومات والتعليم الإلكتروني. ويجب أن يشتمل كل طلب استثناء على المبررات والمزايا المنسوبة إلى الاستثناء من الامتثال للسياسة.

تبلغ فترة الاستثناء من الامتثال للسياسة أربعة أشهر كحد أقصى، ويجب إعادة تقييم هذه المدة واعتماد تمديدها- إذا الزم الأمر. لمدة أقصاها ثلاث فترات متتالية. ولا يجوز الاستثناء من هذه السياسة لأكثر من ثلاث فترات متتالية.

الأدوار والمسؤوليات (مصفوفة المهام RACI):

يوضح الجدول مصفوفة المهام (RACI) التي تحدد الجهة الإشرافية والشخص المسؤول عن مهمة بعينها والجهة التي تستشار أو تبلغ بكل مهمة يجب تنفيذها.

هناك أدوار في هذه السياسة تشترك فيها عدة جهات هي على التوالي: الإدارة، عمادة الاتصالات وتقنية المعلومات، موظف أمن المعلومات، المورد، المالك والمستخدم الموظف والمتعاقد).

الاسم / المسؤوليات	الإدارة	تقنية المعلومات	ضابط أمن المعلومات	المورد	المالك	المستخدم
اعتماد الأنظمة الجديدة أو تعديلها	R,A	C	C		C, I	I
إجراء تقييم للثغرات الأمنية واختبار الاختراق.		C	R,A		C, I	
تحديد الضوابط الأمنية العملية للتخفيف من المخاطر والمهددات التي تواجه الأنظمة المهمة في جامعة حائل		R,A	R,C		C, I	
ضمان حماية نظم المعلومات والبنية التحتية، وفقا للآليات التقنية المحددة من قبل فريق تصميم النظام أو التطبيق.		R,A	C		I	
توفير بيئة تطوير آمنة لحماية سرية المعلومات وسلامتها وتوفرها.		R,A	C		I	
إجراء جميع اختبارات النظام الضرورية (وظيفية، أمنية، إلخ) خلال دورة حياة التطوير.		R,A	C	R,C	I	
تطبيق الضوابط المناسبة لحماية سرية المعلومات الحساسة وسلامتها وصحتها.		R,A	R,C		I	

اتصف مصفوفة راكي (RACI)) الخاصة بتحديد المسؤوليات والأدوار المختلفة التي يشارك بها أعضاء الفريق في إنجاز مهام العمل، وهي مفيدة بشكل خاص في توضيح الأدوار والمسؤوليات عند تنفيذ عمليات تتعدد فيها الوظائف أو الإدارات، يرمز الحرف (R) إلى الموظف الذي ينفذ مهمة من المهام، أما الحرف) ه (A) فيرمز للشخص المسؤول (أو جهة الاعتماد) حيث يوقع هذا الشخص أو يعتمد المهمة المناطة إلى الموظف) * (R أما الحرف (C) فيرمز إلى المستشار الذي يقدم رأياً حول ما هو مراد تنفيذه، ويرمز الحرف (I) إلى الشخص الذي يكون على علم ودراية بالمهمة وهو الذي تصله أحدث المعلومات عن سير المهمة.

الوثائق ذات الصلة:

فيما يلي جميع السياسات والإجراءات ذات الصلة بهذه السياسة:

- سياسة أمن المعلومات
- سياسة تنظيم أمن المعلومات
- سياسة التحكم في الوصول
- سياسة أمن العمليات
- سياسة أمن الاتصالات
- سياسة العلاقات مع الموردين
- سياسة الامتثال
- سياسة إدارة المخاطر
- إجراءات إدارة التغيير
- إجراءات إدارة التصحيح
- إجراءات اقتناء الأنظمة وتطويرها وصيانتها.

الملكية:

هذه الوثيقة مملوكة وتحافظ عليها عمادة تقنية المعلومات والتعليم الإلكتروني بجامعة حائل وهي التي تحافظ عليها.

بيانات السياسة

تقدم الأقسام الفرعية التالية بيانات السياسة في ثلاثة عشر جانبا رئيسيا:

- تحليل متطلبات أمن المعلومات ومواصفاتها.
- تأمين خدمات التطبيقات على الشبكات العامة
- حماية معاملات خدمات التطبيقات.
- سياسة التطوير الأمن.
- إجراءات ضوابط تغيير الأنظمة.
- المراجعة الفنية للتطبيقات بعد تغيير منصة التشغيل.
- ضوابط تغيير حزم البرمجيات.
- مبادئ هندسة النظم الأمنة.
- بيئة التطوير الأمنة.
- الاستعانة بمصادر خارجية لأجل التطوير.
- اختبار أمن النظام.
- اختبار قبول النظام.
- حماية بيانات الاختبار.

تحليل متطلبات أمن المعلومات ومواصفاتها:

١. يجب تحليل متطلبات أمن معلومات الأنظمة الجديدة أو التحسينات التي تجرى للأنظمة الموجودة وإدخال الضوابط اللازمة من خلال عملية رسمية.

٢. في إطار دورة حياة تطوير البرمجيات (مثل التصميم والنشر)، يجب على عمادة الاتصالات وتقنية المعلومات مراعاة الجوانب التالية:

أ. التأكد من أن أنشطة تطوير النظام أو اقتنائه تتم وفقا للشروط والمعايير والإجراءات الموثقة وعمليات جامعة حائل وأفضل ممارساتها.

ب. التأكد من وجود ضوابط كافية (على سبيل المثال، الفصل بين الواجبات) للتخفيف من مخاطر فقدان معلومات من النظام أو حدوث خطأ فيها أو سوء استخدامها.

ج. التأكد من التوثيق الكافي لخطة تأمين أي نظام من الأنظمة وحفظها.

د. التأكد من تحديد وتوثيق وتنفيذ ومراقبة ضوابط أمنية تخص مخاطر محددة تواجه أي نظام من الأنظمة الرئيسة لدعم عمليات تشغيله.

٣. تقوم عمادة تقنية المعلومات والتعليم الالكتروني بالتعاون مع ضابط أمن المعلومات بإجراء تقييم للتهديدات والمخاطر الأمنية أثناء مرحلة المتطلبات عند الإعداد للقيام بتغييرات كبيرة في نظام من الأنظمة أو تنفيذها أو عند الحصول على نظام (جديد) من أجل:

أ. تحديد المتطلبات الأمنية الضرورية لحماية النظام (مثل واجهات التسجيل والمراقبة ومنع تسرب البيانات).

ب. تحديد تصنيف درجة تأمين النظام.

تأمين خدمات التطبيقات على الشبكات العامة:

١. يجب حماية جميع المعلومات المتعلقة بخدمات التطبيقات التي تمر عبر الشبكات العامة من أي نشاط احتيالي أو نزاع على عقود أو إفشاء وتعديل غير مصرح بهما. لذا يجب أن تؤخذ الضوابط الأمنية التالية في الحسبان.

أ. طريقة المصادقة الآمنة (مثل تشفير المفتاح العمومي أو التوقيعات الرقمية).

ب. متطلبات الصمود أمام الهجمات (على سبيل المثال، رفض الخدمة).

ج. عمل اتفاقية توثيق مع الموردين (إذا لزم الأمر).

٢. يجب حماية سلامة المعلومات المتوفرة على نظام متاح للجمهور (على سبيل المثال، موقع جامعة حائل) من أي تعديل غير مصرح به. لذا الأشياء التالية - على سبيل المثال لا الحصر - يجب أن توضع في الحسبان.

أ. يطور موقع جامعة حائل الإلكتروني ولا يقوم بصيانته إلا أفراد مؤهلون تأهيلاً جيداً ولديهم تصريح صحيح بذلك.

ب. يجب توثيق جميع التغييرات التي تتم على الموقع الإلكتروني ومعالجتها من خلال إجراءات إدارة التغيير الخاصة بالجامعة.

ج. يجب تقديم رسالة تحذير مناسبة على موقع الويب تفيد بأنه لا يجوز نسخ أي معلومات أو إعادة إنتاجها دون وضع إشعارات حقوق الطبع والنشر الأولية.

د. يجب التحقق من المعلومات التي تم الحصول عليها من مصادر الإنترنت قبل استخدامها لأغراض أعمال حائل.

حماية معاملات خدمات التطبيقات:

١. يجب حماية جميع المعلومات المتعلقة بالمعاملات المتداولة عبر الإنترنت لمنع بثها بطريقة غير مكتملة أو توجيهها في المسار الخطأ أو الإفصاح عنها بطريقة غير مصرح بها أو تغيير الرسالة غير المصرح بها أو إعادة إنتاجها أو إرسالها بطريقة غير مصرح بها.

٢. بالنسبة لجميع معاملات خدمات التطبيقات، على جميع الأطراف مراعاة ما يلي:

أ. التثبت من التحقق الأمن.

ب. تشفير مسار الاتصالات.

ج. الحفاظ على خصوصية البيانات.

د. سرية المعاملات.

سياسة التطوير الأمن:

١. يجب على عمادة تقنية المعلومات والتعليم الإلكتروني تحديد وتنفيذ القواعد التي تحكم تطوير البرمجيات داخل جامعة حائل حيث يشمل ذلك، على سبيل المثال لا الحصر ما يلي بالنسبة لجميع معاملات خدمات التطبيقات، على جميع الأطراف مراعاة ما يلي:

أ. اتباع منهجية آمنة لتطوير البرمجيات.

ب. تطبيق ممارسات تشفير آمنة (مثل المعايير وخطوط الأساس ومراجعة الرموز).

ج. تحديد المشاكل الأمنية ومعالجتها (مثل الثغرات الأمنية).

٢. يجب على عمادة تقنية المعلومات والتعليم الإلكتروني تعيين مطورين ومبرمجين مؤهلين ومدربين أكفاء لتصميم شفرة للبرنامج واختباره والتحقق منه وفقا لأفضل الممارسات الدولية.

إجراءات التحكم في تغيير النظام:

١. يجب على عمادة تقنية المعلومات والتعليم الإلكتروني التأكد من التوثيق والتنفيذ الكافي للإجراءات الرسمية المتعلقة بمراقبة تغيير النظام.

٢. يجب أن تضمن عمادة تقنية المعلومات والتعليم الإلكتروني اختبار جميع التغييرات في الأنظمة وتسجيلها وتحديثها وصيانتها بدقة. وهذا يشمل -على سبيل المثال لا الحصر- ما يلي:

أ. إخضاع جميع التغييرات أو تثبيت البرامج الجديدة لاختبار في بيئة اختبار.

ب. فصل بيئة الاختبار تماما عن بيئة الإنتاج.

ج. تنفيذ التغييرات في الوقت المناسب بحيث لا يؤثر ذلك سلبا على سير أعمال جامعة حائل.

المراجعة الفنية للتطبيقات بعد إحداث تغييرات في منصة التشغيل:

١. يجب أن تخضع الإصدارات الجديدة أو الإصدارات المختلفة لمنصة التشغيل لعملية إدارة تغيير محددة وفقا لمتطلبات أعمال جامعة حائل قبل تثبيتها.

٢. جب إجراء مراجعة تقنية لضوابط التطبيقات وسلامتها قبل جميع عمليات النشر غير الطارئة في الإنتاج. يجب أن تكون الضوابط متوافقة مع هيكل أمن المعلومات كما يجب أن توافق عليها الإدارة كجزء من عملية إدارة التغيير الرسمية.

٣. يجب تخطيط متطلبات سعة النظام قبل إدخال تطبيق عمل مهم جديد، ويجب مراجعة هذه المتطلبات أثناء القيام بتطوير النظام والتطبيقات. كما يجب اتخاذ الاحتياطات اللازمة لتجنب أي مشاكل في التطبيقات أو الأنظمة تتعلق بتوفرها.

القيود المفروضة على التغييرات في حزم البرمجيات:

١. يجب أن يكون توثيق إدارة التغيير وتحليل التأثير على أساس مستمر لتغييرات التطبيق جزءا من دورة حياة تطوير النظام وفقا لمتطلبات أعمال جامعة حائل.

٢. يجب عدم تشجيع تعديل حزم البرامج. فحزم برامج البائعين يجب أن تستخدم دون أي تعديل إلى أقصى حد ممكن وعملي.

٣. يجب تنفيذ عملية إدارة تصحيح البرمجيات لضمان مسألة المواكبة والتحديث مع الأخذ في الاعتبار الأشياء التالية:

أ. تحديث البرمجية باستخدام أخر التصحيحات والضبطيات المقدمة من البائع أو المعتمدة منه لإدارة المخاطر.

ب. تنفيذ إجراءات تقوية تكوين الجهاز لحماية البرمجية من التهديدات الأمنية.

تأمين مبادئ هندسة النظم:

١. يجب على عمادة تقنية المعلومات والتعليم الإلكتروني تحديد وتوثيق وصيانة وتنفيذ مبادئ هندسة النظم الأمنة في جميع طبقات التصميم المعماري (مثل الأعمال والبيانات والتطبيقات والتقنية). كما يجب مراجعة هذه المبادئ وتحديثها بشكل منتظم.

٢. يجب إجراء مراجعات مناسبة للتحقق من تطبيق ضوابط المدخلات، والمخرجات، والمعالجة على التطبيقات وقاعدة البيانات من أجل ما يلي:

أ. اعتماد بيانات المدخلات والمخرجات.

ب. كشف فساد المعلومات سواء كان هذا الفساد ناتج عن خطأ في المعالجة أو ناجم عن أفعال متعمدة.

ج. اعتماد المعالجة الصحيحة والملائمة للمعلومات المخزنة.

٣. تضمن عمادة تقنية المعلومات والتعليم الإلكتروني صحة وسلامة إدخال البيانات إلى الأنظمة من خلال ما يلي:

أ. قصر الحقول على قبول مديات (جمع مدى) محددة من البيانات (على سبيل المثال، تحديد القيم التي خارج المدى أو الحدود العليا والسفلى لحجم البيانات).

ب. التأكد من عدم وجود أحرف غير صالحة في حقول البيانات.

ج. نجعل الحقول الرئيسة إلزامية.

د. التحقق من مقبولية بيانات الإدخال باستخدام قواعد العمل.

ه. الحماية من الهجمات الشائعة (على سبيل المثال، تجاوزات المخزن المؤقت، أو هجمات الحرمان من الخدمات (DoS)، أو الهجمات الموزعة للحرمان من الخدمة (DDoS)

و. استخدام أرصدة التحكم للتحقق من اكتمال الإدخال والمعالجة

ز. على عمادة تقنية المعلومات والتعليم الإلكتروني تحديد وتوثيق مسؤوليات كل فريق فني يشارك في عمليات إدخال البيانات والمخرجات (مثل مطوري النظم ومحللها ومصمميها).

بيئة التنمية الآمنة:

ا. على عمادة تقنية المعلومات والتعليم الإلكتروني أن تؤسس بيئة تطوير آمنة (تشمل الأشخاص والعمليات والتقنية) في إطار متطلبات دورة حياة تطوير البرمجيات، على أن تغطي هذه المتطلبات الجوانب التالية:

أ. حساسية البيانات.

ب. قابلية السياسات الداخلية واللوائح الخارجية للتطبيق.

ج. تنفيذ التدابير الأمنية.

د. الفصل بين بيئات التطوير المختلفة.

ه. مستوى طرق الوصول والتحقق من هوية من يريد الوصول).

و. التحكم في التغيير.

ز. نقل البيانات من بيئة التطوير واليها.

الاستعانة بمصادر خارجية لأجل التطوير:

ا. تشمل شروط الاستعانة بمصادر خارجية لتطوير النظام ما يلي على سبيل المثال لا الحصر:

أ. الامتثال لمنهجية مقبولة لتطوير وصيانة النظام.

ب. مراقبة الأنشطة والإشراف عليها بدقة (مثل إجراء الاختبارات وقبول المستخدم).

اختبار تأمين النظام:

ا. تقوم عمادة تقنية المعلومات والتعليم الإلكتروني باختبار ميزات ووظائف الأمن داخل نظام ما أثناء عمليات التطوير مثل:

أ. التحكم في الوصول وطرق التحقق من هوية المستخدم)

ب. تحديد الامتيازات وإدارتها.

ج. النسخ الاحتياطي واستعادة البيانات.

د. تشفير البيانات وخصوصيتها.

اختبار قبول النظام:

ا. يجب أن تضمن عمادة تقنية المعلومات والتعليم الإلكتروني أن متطلبات ومعايير قبول الأنظمة الجديدة محددة بوضوح ومتفق عليها وموثقة ومختبرة. كما يجب النظر في المعايير التالية، على سبيل المثال لا الحصر:

أ. متطلبات الأداء وسعة النظام.

ب. خطأ الاسترداد، إجراءات إعادة التشغيل وخطط الطوارئ.

ج. إعداد واختبار إجراءات التشغيل الروتينية.

د. وجود مجموعة متفق عليها من الضوابط الأمنية.

ه. ترتيبات استمرارية العمل.

و. إثبات أن تركيب الأجهزة الجديدة لا يؤثر سلبا على أنظمة التحكم والأتمتة الحالية، لا سيما في أوقات ذروة المعالجة (على سبيل المثال، في النهار).

ز. دليل على الأخذ في الاعتبار عدم تأثير الأجهزة الجديدة على الأمن العام لأنظمة جامعة حائل.

ح. التدريب على تشغيل أو استخدام المعدات الجديدة.

ط. ضمانات الصيانة ودعمها.

حماية بيانات الاختبار:

ا. يجب تنفيذ جميع الضوابط الأمنية المطبقة في بيئة الإنتاج على بيئة الاختبار لضمان الحماية المناسبة لبيانات الاختبار وذلك بأخذ الأشياء التالية في الاعتبار:

أ. منح إذن الوصول «للقراءة» و «النسخ» فقط في الحالات الخاصة والموافق عليها مسبقا حيث يكون الوصول إلى بيانات الإنتاج مطلوبا لتطوير أو اختبار تطبيقات أو أنظمة العمل، ويتم إلغاء الإذن عند الانتهاء بنجاح من المهمة.

ب. الحصول على إذن منفصل في كل مرة يتم فيها نسخ بيانات الإنتاج لأجل بيئة التطوير أو لأجل بيئة الاختبار.

ج. مسح أي نسخ من معلومات الإنتاج المستخدمة في بيئة التطوير أو بيئة اختبار فور الانتهاء من هذه المهام.