المملكة العربية السعودية

سياسة ضبط الدخول
في الجامعة العربية المفتوحة

الاعتماد	2021

المحتويات :

مادة(1) : تسمية

تسمى هذه السياسة "**سياسة ضبط الدخول في الجامعة العربية المفتوحة**".

مادة(2) : تعريفات

يكون للكلمات والمصطلحات الآتية حيثما ترد في هذه اللائحة المعاني الواردة أدناه، ما لم يدل السياق على خلاف ذلك:

الجامعة	الجامعة العربية المفتوحة في المملكة العربية السعودية
الرئيس	رئيس الجامعة في المملكة العربية السعودية
مالك الأصل	فرد أو مجموعة جرى تكليفهم من قبل إدارة الجامعة بالحفاظ على سرية و أمن و توفر المعلومات و من ضمن عملهم مراجعة الصلاحيات وتصنيف الأصول
الاصول	المعلومات التي لها قيمة في الجامعة مثل الشبكات والاجهزة زالمعلومات والبرمجيات والوسائط ونظم المعلومات

.

مادة (3) : المقدمة

تهدف الجامعة العربية المفتوحة إلى توفير متطلبات الأمن السيبراني المتعلقة باستخدام أنظمة الجامعة العربية المفتوحة وتوثيق الاجراءات الرسمية لضبط دخول المستخدمين إلى الأصول المعلوماتية والتقنية للجامعة ومنع دخول الاشخاص الغير مصرح لهم إلى انظمة الجامعة للحفاظ على المعلومات.

وتهدف هذه السياسة إلى الالتزام بمتطلبات وضوابط الأمن السيبراني الصادرة من الهيئة الوطنية للامن السيبراني وهي مطلب تشريعي في الضابط رقم ٢-2 من الضوابط الأساسية للأمن السيبراني(ECC-1:2018) .

تنطبق هذه السياسة على جميع الهويات والحسابات الخاصة بالمستخدمين بدء من التسجيل المبدئي للمستخدمين وصولًا إلى إلغاء صلاحيات الدخول للمستخدمين في حال الاحتياج لذلك وتطبق على جميع مستخدمي الأصول المعلوماتية والانظمة بما في ذلك الإدرايين والأكاديميين الدائمين و المؤقتين في الجامعة.

إن أي انتهاك لهذه السياسة يعرض صاحب المخالفة إلى إجراءت تأديبية حسب الإجراءات المُتبعة في الجامعة العربية المفتوحة.

مادة (4) : أهداف السياسة

4-1 ضبط وتنظيم عمليات الدخول على الحسابات بناء على متطلبات العمل والمتطلبات الامنية.

4-2توثيق الإجراءات الرسمية لضبط دخول المستخدمين.

4-3حماية سرية وسلامة وتوفر المعلومات المخزنة على شبكة وانظمة الجامعة

مادة(5) : بنود سياسة ضبط الدخول

5-1 إنشاء وتعديل و إيقاف حسابات المستخدمين

5-1-1- يخصص لكل مستخدم من مستخدمي نظم المعلومات اسم مستخدم محدد وصلاحيات محددة بناء على مالك الاصل ويمنع تبادل اسماء المستخدمين بين المستخدمين.

5-1-2 يزود كل مستخدم ببيانات الدخول على أن تتطلب الصلاحية ما لايقل عن عامل واحد من عوامل المصادقة (مثل كلمة السر- رقم رمز المطابقة)

5-1-3 يمنع التفويض والتعديل على الصلاحيات الخاصة بالمستخدمين أوإلغاء دخول المستخدمين دون إذن من الإدارة المختصة.

5-1-4 يطبق مبدأ الفصل بين الواجبات عند إنشاء الحسابات وعملية تحديد الصلاحيات.

5-1-5 يجب عند إدارة وتحديد صلاحيات المستخدمين مراعاة التالي من مبادئ التحكم بالدخول والصلاحيات:

5-1-5-1 – مبدأ الحاجة إلى المعرفة والاستخدام.

5-1-5-2- مبدأ فصل المهام.

5-1-5-3- مبدأ الحد الادنى من الصلاحيات والامتيازات.

5-1-6 يجب إيقاف صلاحيات المستخدمين عند انتهاء عقدهم مع الجامعة (تقاعد-استقالة-فصل) حيث توقف الخدمات في آخر يوم عمل لهم.

5-1-7 عند الاشتباه باتخاذ الموظف إجراءات تضر بالجامعة قبل أو عند إنهاء خدمته توقف صلاحيات دخوله للأنظمة قبل منحه إشعار إنهاء الخدمة.

5-1-7 يجب تعديل صلاحيات المستخدم عند حدوث أي تغيير في المهام المكلف بها وإعطائه صلاحيات تتناسب مع مهامه.

5-2 إدارة كلمات المرور الخاصة بالمستخدمين:

5-2-1- يجب تفعيل المصادقة لجميع أنظمة الجامعة من خلال كلمات المرور قبل السماح للمستخدم بالدخول .

5-2-2- تعطيل حساب المستخدم بعد 3 محاولات فاشلة للدخول.

5-2-3 يجب تغيير كلمة المرور في حال الشك بانكشافها وإبلاغ إدارة تقنية المعلومات.

5-2-4 - يجب فرض تغيير كلمة المرور بصفة دورية كل 180 يوم على الأقل وعدم تكرار كلمة السر السابقة.

5-2-5- يجب إعادة تفعيل كلمة المرور عن طريق إدارة تقنية المعلومات بعد التحقق رسميًا من هوية المستخدم وتعثر استعادة كلمة المرور آليًا.

5-2-6 يجب الالتزام باستخدام المعايير المطلوبة عند اختيار كلمة السر وطولها وتعقيدها.

5-2-7 يجب الحفاظ على سرية كلمة المرور وعدم التصريح عنها بأي طريقة (مثال عن طريق الهاتف أو الايميل أو الكتابة على ورق ...)

5-3 إدارة الامتيازات:

5-3-1 يجب تحديد ضوابط الدخول على الحسابات ذات الامتيازات العالية كمسؤولي الأنظمة ومسؤولي الشبكات وتطبيق ضوابط مشددة عليها وأخذ الموافقة.

5-3-2 استخدام الحسابات ذات الامتيازات عالية المستوى عند الحاجة إلى هذه الامتيازات الوظيفية ولا تسخدم في مهام المستخدم الروتينية التي لا تتطلب استخدامها.

5-303 يجب تدريب مستخدمي الحسابات ذات الامتيازات عالية مستوى قبل استخدام الحساب.

5-3-4 يجب توفير حسابات خاصة لجميع مستخدمين الحسابات ذات الامتيازات عالية المستوى تستخدم لأداء مهامهم الروتينية.

5-3-5 يجب حماية وتغيير كلمة السر بصفه دورية.

5-4 مراجعة صلاحيات دخول المستخدمين:

5-4-1 يجب على قسم تقنية المعلومات ومالك الاصول مراجعة صلاحيات المستخدمين بشكل سنوي.

5-4-2 في حال رصد أي سوء استخدام في صلاحيات الدخول الممنوحة تقيّد هذه الصلاحيات.

مادة (6) : الاستثناءات

1. يجب على جميع العاملين بالجامعة الالتزام بهذه السياسات و أي إستثناء في هذه السياسة الحصول على اذن من ادارة تقنية المعلومات .

المادة (7) : العقوبات

إن أي انتهاك لهذه السياسة يعرض صاحب المخالفة إلى إجراء تأديبي؛ حسب الإجراءات المُتبعة في الجامعة العربية المفتوحة.

المادة (8) : أحكام عامة

يبت مجلس الجامعة في الحالات التي لم يرد فيها نص في السياسة بعد رفع الحالة من قبل إدارة تقنية المعلومات.