STARDOM UNIVERSITY

سياسات أنظمـة ولوائح
دليل
سياسة ضبط الدخول

صادرة بموجب المادة (16) من السياسـات
اللوائـح و الأنظمة الأكاديمية لعام 2024

إعتماد مجلس إدارة الجامعة رقم (65)

2024/07

سياسة
ضبط الدخول
الخاصة بجامعة ستاردوم

المقدمة

تُعد جامعة ستاردوم من الجامعات الإلكترونية الرائدة التي تعتمد على نظام التعليم الإلكتروني والتعليم المدمج للعملية التعليمية. يحتوي هذا النظام على العديد من المعلومات والبيانات الخاصة بالموظفين والطلاب والأبحاث العلمية، والتي قد تتعرض للاختراق وسوء الاستخدام، مما يشكل انتهاكًا خطيرًا لخصوصية الطالب وبياناته. من هنا، برزت الحاجة إلى وضع سياسة ضبط الدخول لضمان الحماية الكافية للمعلومات الشخصية وتوفير طريقة سهلة وسريعة لتسجيل الدخول لنظام الطالب.

يهدف هذا الدليل إلى توفير متطلبات الأمن السيبراني لتقليل المخاطر المرتبطة باستخدام أنظمة جامعة ستاردوم وأصولها، وحمايتها من التهديدات الداخلية والخارجية. يركز الدليل على المحافظة على سرية المعلومة وسلامتها وتوافرها، بالإضافة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وذلك كجزء من الضوابط الأساسية للأمن السيبراني.

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية والخدمات المقدمة عن طريق الإنترنت، بما في ذلك المواقع الإلكترونية، تطبيقات الويب، تطبيقات الهواتف الذكية واللوحية، البريد الإلكتروني، والدخول عن بعد. تنطبق هذه السياسة على جميع العاملين في الجامعة، سواء العاملين المباشرين أو غير المباشرين، وكذلك على موظفي الجهات الخارجية المسموح لهم باستخدام المعلومات والأنظمة التي تمتلكها الجامعة.

أهداف السياسة

- تقليل المخاطر السيبرانية وما يترتب عليها من انتهاك للخصوصية.
- وضع ضوابط تحكم عمليات الدخول إلى الحسابات بناءً على متطلبات العمل والمتطلبات الأمنية.
- توثيق الإجراءات الرسمية لضبط دخول المستخدمين.
- المحافظة على المعلومات وحماية سريتها وسلامتها وتوافرها على شبكة وأنظمة الجامعة.

بنود سياسة ضبط الدخول

إنشاء وتعديل الحسابات

- تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لإدارة تسجيل الدخول، وتحديد الهوية والصلاحيات بناءً على اسم المستخدم وكلمة المرور.
- إنشاء حسابات مميزة وغير مكررة لضمان التعرف على هويات المستخدمين أثناء استخدامهم لأنظمة الجامعة.
- تقوم إدارة الأنظمة بتحديد ومصادقة جميع المستخدمين بشكل فريد قبل منحهم الوصول إلى النظام.
- إجراء مراجعات دورية لحسابات المستخدمين وإرفاق رقم مرجعي فريد مع كل طلب إنشاء حساب للمستخدمين لضمان تتبعهم.
- توثيق الإجراءات للتعامل مع حسابات الخدمة والتأكد من إدارتها بشكل آمن بين التطبيقات والأنظمة.
- السماح بإنشاء حسابات وصناديق بريد إلكترونية مشتركة بشرط تحديد مالك واحد لكل حساب لضمان التتبع والمسؤولية.
- إيقاف حسابات الطلبة القدامى أو المستقيلين وسحب جميع صلاحياتهم.
- تعديل صلاحيات الموظفين بناءً على التغييرات الوظيفية الموكلة إليهم.

إدارة كلمة المرور للمستخدمين

- منع مشاركة كلمة المرور عبر أي وسيلة، بما في ذلك البريد الإلكتروني والاتصالات الصوتية.
- اختيار كلمات مرور تختلف عن تلك المستخدمة في الحسابات الشخصية.
- تعطيل الحساب بعد ثلاث محاولات دخول فاشلة.
- استخدام أنظمة التحقق من الهوية متعدد العوامل أو المصادقة المزدوجة للبيانات الحساسة.
- اتباع معايير قياسية لاختيار اسم المستخدم وكلمة المرور من حيث الطول والتعقيد.
- السماح للمستخدمين بتغيير كلمات المرور الخاصة بهم.
- عدم تخزين كلمات المرور كنصوص واضحة، بل تشفيرها.
- حفظ عمر كلمة المرور وتاريخها ومنع استخدام نفس كلمة المرور السابقة.
- إجبار المستخدمين على تغيير كلمات المرور المؤقتة عند أول دخول لهم.

إدارة الامتيازات

- قصر الدخول إلى أنظمة التشغيل وتطبيقاتها على مديري النظم المسؤولين وفريق الدعم.
- منح الامتيازات للمستخدمين بناءً على تفويض رئيسهم وبما يتناسب مع مهامهم الوظيفية.
- تقييم امتيازات المستخدمين بشكل دوري واتخاذ الإجراءات اللازمة بناءً على نتائج التقييم.
- استخدام الحسابات ذات الامتيازات العالية فقط عند الحاجة، وتجنب استخدامها في الإجراءات الروتينية.
- تدريب مستخدمي الحسابات ذات الامتيازات العالية وتوعيتهم بحساسية حساباتهم والمسؤوليات المترتبة على سوء الاستخدام.
- حماية وتغيير كلمات مرور الحسابات ذات الامتيازات بصورة دورية.
- إنشاء وتفعيل حسابات المستخدمين التابعين للجامعة أو المتعاقدين لفترات زمنية محددة، وحذفها عند انتهاء الحاجة إليها.
- إيقاف حسابات الموظفين في حالة صدور عقوبة تأديبية بحقهم قبل إشعارهم بذلك.
- منع استخدام الحسابات المشتركة للوصول إلى الأصول المعلوماتية والفنية وتقييدها بصلاحيات محددة.

مراجعة صلاحيات تسجيل الدخول

- مراجعة حقوق وامتيازات وصول المستخدمين مرة واحدة على الأقل في السنة.
- تقييد الامتيازات في حال الكشف عن أي سوء استخدام.
- تسجيل جميع محاولات الوصول الفاشلة والناجحة ومراجعتها بشكل دوري.

الاستثناءات

- يجب على جميع العاملين بالجامعة الالتزام بهذه السياسات. ويجب الحصول على إذن من إدارة تقنية المعلومات لأي استثناء.
- الرجوع إلى إدارة تقنية المعلومات وطلب تصريح مسبق قبل إدخال أي طرف ثالث وإعطائه حق الوصول لنظام الجامعة.

العقوبات

- في حال حدوث أي انتهاك متعمد أو نتيجة إهمال، يتم اتخاذ الإجراءات التأديبية المناسبة وفقًا للوائح والأنظمة المعمول بها في الجامعة.