

المملكة العربية السعودية

جمعية التنمية الأسرية بالمنطقة الشرقية (وثام)
مسجلة بوزارة الموارد البشرية والتنمية الاجتماعية
رقم (496)



سياسة ضبط الدخول

ديسمبر - 2022 م

تاريخ الاصدار:

001

رقم الاصدار:

مقدمة

تهدف هذه السياسة لوضع المبادئ التي تستند إليها ضوابط التحكم في الوصول لأجهزة وبيانات الجمعية.

السياسة

1. إنشاء وإيقاف حسابات المستخدمين

- يتم تقديم طلبات الحصول على بيانات الدخول إلى شبكة الجمعية فقط من الموارد البشرية. تخضع جميع الطلبات الى عمليات معالجة بناء على الإجراءات الرسمية المعتمدة والتي تضمن تطبيق الضوابط الأمنية المناسبة.
- تخصص الجمعية لكل مستخدم اسم مستخدم فريد مرتبط بمنسوب محدد وليس بمهمله أو مسمى وظيفي. كما ويمنع تبادل أسماء المستخدمين بين المنسوبين. ويحظر إنشاء حسابات المستخدمين العامة، مثل الحسابات الفردية المستخدمة من قبل مجموعة من الأشخاص لأنه يصعب تحديد المسؤوليات من خلالها.
- في حالة استقالة أو إيقاف المستخدم عن العمل، يجب على الموارد البشرية إشعار قسم التنقية فوراً ليتم سحب صلاحيات الدخول إلى النظم فور إنهاء خدماته في آخر يوم عمل له في الجمعية. في حالات محددة واستثنائية، عند الاشتباه بأن الموظف قد يتخذ إجراءات تضر بالجمعية قبل أو عند إنهاء خدمته، يتم الموافقة على طلب سحب صلاحيات دخوله للأنظمة قبل منحه إشعار إنهاء الخدمة. وتطبق هذه السياسة على الموظفين ذوي صلاحيات الدخول عالية المستوى مثل مشرفي المجال.
- يجب تعليق حسابات المستخدمين أو تعطيلها فقط ويمنع إلغائها. وينبغي للجمعية عدم تخصيص حسابات المستخدمين والتي سبق استخدامها لمستخدمين جدد وذلك منعا لحدوث اشتباه في حالة التدقيق لاحقاً.

2. إتاحة حسابات دخول المستخدمين

- يجب منح كل مستخدم حقوق دخول النظام التي تتناسب مع المهام المتوقع تنفيذها. وبصفة عامة يعتمد ذلك على الأدوار، حيث يتوجب إنشاء مجموعات مستخدمين ترتبط بصلاحيات دخول محددة ويتم إضافة حساب المستخدم إليها بناء على الدور الوظيفي له.
- يجب أن تتوافق ادوار المجموعات مع متطلبات العمل، وأي تغيير يحصل على هذه الأدوار يتم ضبطه والتحكم به والموافقة عليه عبر عملية إدارة التغيير.
- لا ينبغي منح المستخدمين صلاحيات مخصصة خارج تلك المحددة للمجموعة، وفي حال طلب صلاحيات إضافية يتم تقديم طلب رسمي وتطبيق عمليات ادارة التغيير.

3. إزالة أو تعديل حقوق الدخول

- ينبغي سحب أو تعديل حقوق دخول المنسويين فور حدوث تغيير على الدور المناط بهم. وفي حالة تكليف المنسوب بدور جديد إضافة إلى الأدوار الحالية المناطة له، يتم طلب حقوق دخول باتباع عمليات إدارة التغيير، مع ضرورة الإشارة إلى المهام المناط إليه حالياً والجديدة مع بعض وذلك لتطبيق مبدأ الفصل بين المهام.
- يمنع تحت أي ظرف من الظروف قيام المسؤول بتعديل الصلاحيات الخاصة به.

4. إدارة حقوق الدخول ذات الامتيازات

- يجب تحديد حقوق الدخول ذات الامتيازات عالية المستوى كمسؤولي الأنظمة ومسؤولي الشبكة وتطبيق ضوابط مشددة عليها. وبصفة عامة، يمنع على الفنيين مثل موظفي الدعم الفني استخدام صلاحيات الدخول ذات الامتيازات لمتابعة المهام اليومية المتعلقة بحسابات المستخدمين إلا عند الحاجة لهذه الامتيازات الإضافية، وفيما عدا ذلك يتم إنشاء حسابات منفصلة لمسؤولي الأنظمة للقيام بمهامهم.
- ويجب أن تكون هذه الحسابات محددة لشخص بعينه. ولا ينبغي استخدامها كحسابات عامة لأن معلومات المستخدم فيها غير كافية.
- ينبغي أن يقتصر منح صلاحيات الدخول على مستوى «مسؤولي الأنظمة» للأفراد الذين تتطلب طبيعة مهامهم هذه الصلاحيات وبعد خضوعهم لتدريب كافي لتقدير الآثار المترتبة على هذا الاستخدام. كما ينبغي تجنب استخدام حسابات الدخول ذات الامتيازات الخاصة لتنفيذ الأعمال الروتينية قدر الإمكان. كما ويجب حماية كلمة المرور المستخدمة وتغييرها بصورة منتظمة في الحالات التي لا مفر من استخدام الحسابات ذات الامتيازات فيها.

5. مراجعة حقوق دخول المستخدم

- يتوجب على مالكي الأصول والأنظمة بصورة منتظمة (مرة سنوياً على الأقل) مراجعة من حاول الوصول إلى مناطق مسؤوليتهم ومستوى صلاحيات الدخول، وذلك من أجل تحديد التالي:
- الأشخاص غير المصرح لهم بالدخول (مثل من ترك العمل في الجمعية).
- حسابات المستخدمين التي سجلت وصولاً أكثر مما هو مطلوب بمهام الوظيفة المناطة بهم.
- حسابات المستخدمين الذين تم تخصيص أدوار غير صحيحة لهم.

- حسابات المستخدمين التي لم تقدم تحققا كافيا مثل الحسابات العامة او المشتركة.
- اي قضايا أخرى لا تتفق مع السياسة.
- يتوجب تنفيذ هذه المراجعة بناء على الاجراءات الرسمية مع ضرورة تحديد وتنفيذ اي اجراءات تصحيحية.

والله الموفق ،،

رئيس مجلس الإدارة:

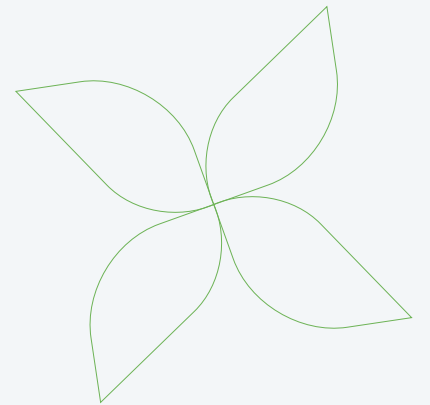


فؤاد بن عيسى العيسى





وثام، لتمكين الأسرة



920012571



@weaam.org