Password Policy and Guidelines

سياسة وإرشادات كلمة المرور

Policy Statement

All individuals are responsible for safeguarding their system access login and password credentials and must comply with the password parameters and standards identified in this policy. Passwords must meet the complexity requirements outlined and must not be shared with or made available to anyone in any manner that is not consistent with this policy and procedure.

بيان السياسة

يتحمل جميع الأفراد مسؤولية حماية بيانات تسجيل الدخول وكلمة المرور الخاصة بهم للوصول إلى النظام ويجب أن يلتزموا بمعايير كلمة المرور المحددة في هذه السياسة.
يجب أن تفي كلمات المرور بمتطلبات التعقيد الموضحة ويجب عدم مشاركتها أو إتاحتها لأي شخص بأي طريقة لا تتوافق مع هذه السياسة والإجراءات.

Reason for Policy

Assigning unique user logins and requiring password protection is one of the primary safeguards employed to restrict access to RAKAA data to only authorized users. If a password is compromised, access to information systems can be obtained by an unauthorized individual. Individuals with password credentials are responsible for safeguarding against unauthorized access to their account, and as such, must conform to this policy in order to ensure passwords are kept confidential and are designed to be complex and difficult to breach.

سبب السياسة

يعد تعيين حسابات فريدة للمستخدم ووجود الحاجة لحماية كلمة المرور أحد الضمانات الأساسية المستخدمة لتقييد الوصول إلى بيانات المدرسة للمستخدمين المصرح لهم فقط. إذا تم اختراق كلمة المرور ، يمكن الوصول إلى أنظمة المعلومات بواسطة فرد غير مصرح له.
الأفراد الذين لديهم بيانات كلمة المرور مسؤولون عن الحماية ضد الوصول غير المصرح به إلى حساباتهم ، وعلى هذا النحو ، يجب أن يلتزموا بهذه السياسة من أجل ضمان الحفاظ على سرية كلمات المرور وأن تكون مصممة لتكون معقدة ويصعب اختراقها.

1. Individual Responsibilities

Individuals are responsible for keeping passwords secure and confidential. As such, the following principles must be adhered to for creating and safeguarding passwords:

- Passwords must be changed immediately upon issuance for the first use. Initial passwords must be securely transmitted to the individual, either via the IT Department or Human Resources.
- Passwords must never be shared with another individual for any reason or in any manner not consistent with this policy.
- Employees including admin, teachers, and supervisors as well as students and other personnel, must never ask anyone else for their password. If you are asked to provide your password to an individual or sign into a system and provide access to someone else under your login, you are obligated to report this to the IT department.
- Passwords must never be written down and left in a location easily accessible or visible to others.

1. المسؤوليات الفردية

يتحمل الأفراد مسؤولية الحفاظ على أمان وسرية كلمات المرور. على هذا النحو، يجب الالتزام بالمبادئ التالية لإنشاء كلمات المرور وحمايتها:

- يجب تغيير كلمات المرور فور إصدارها لأول استخدام. يجب نقل كلمات المرور الأولية بشكل آمن إلى الفرد، إما عبر قسم تكنولوجيا المعلومات أو الموارد البشرية.
- يجب عدم مشاركة كلمات المرور مطلقًا مع أي شخص آخر لأي سبب أو بأي طريقة لا تتفق مع هذه السياسة.
- يجب ألا تطلب الموظفات، بمن فيهم المسؤولات والمعلمات والمشرفات وكذلك الطلبة والموظفات الأخريات، من أي شخص آخر كلمة المرور الخاصة بهم. إذا طُلب منك تقديم كلمة المرور الخاصة بك إلى فرد آخر (أي شخص) أو تسجيل الدخول إلى النظام وتوفير الوصول إلى شخص آخر بموجب تسجيل الدخول الخاص بك ، فأنت ملزم بإبلاغ قسم تكنولوجيا المعلومات بذلك.
- يجب عدم تدوين كلمات المرور مطلقًا وتركها في مكان يسهل الوصول إليه أو رؤيته للآخرين.

- Individuals must never leave themselves logged into an application or system where someone else can unknowingly use their account.
- يجب ألا يترك الأفراد أنفسهم مسجلين للدخول إلى تطبيق أو نظام حيث يمكن لشخص آخر استخدام حسابه دون علمه.

- In the event that a password needs to be issued to a remote user or service provider, the password must never be sent without the use of proper safeguards (e.g., do not send passwords through email without encryption).
- في حالة الحاجة إلى إصدار كلمة مرور لمستخدم بعيد أو مزود خدمة ، يجب عدم إرسال كلمة المرور مطلقًا دون استخدام وسائل الحماية المناسبة (على سبيل المثال ، لا ترسل كلمات المرور عبر البريد الإلكتروني بدون تشفير).

- If a password needs to be shared for servicing, IT department should be contacted for authorization and appropriate instruction.
- إذا كانت هناك حاجة إلى مشاركة كلمة المرور من أجل الصيانة ، فيجب الاتصال بقسم تكنولوجيا المعلومات للحصول على التفويض والتعليمات المناسبة.

- Passwords must be unique and different from passwords used for other personal services (e.g., banking).
- يجب أن تكون كلمات المرور فريدة ومختلفة عن كلمات المرور المستخدمة للخدمات الشخصية الأخرى (مثل الخدمات المصرفية).

- Passwords must meet the complexity requirements outlined in this policy.
- يجب أن تلبي كلمات المرور متطلبات التعقيد الموضحة في هذه السياسة.

- Passwords must be changed regularly, as outlined in this policy, at the regularly scheduled time interval or sooner if there is suspicion of a compromise.
- يجب تغيير كلمات المرور بانتظام ، كما هو موضح في هذه السياسة ، في الفاصل الزمني المجدول بانتظام أو قبل ذلك إذا كان هناك اشتباه في وجود اختراق

- In the event a breach or compromise is suspected, the incident must be reported to IT department immediately.
- في حالة الاشتباه في وجود خرق، يجب إبلاغ قسم تكنولوجيا المعلومات بالحادث على الفور.

2. Password Requirements

The following parameters indicate the minimum requirements for passwords for all individual accounts where passwords are:

2. متطلبات كلمة المرور

تشير النقاط التالية إلى الحد الأدنى من متطلبات كلمات المرور لجميع الحسابات الفردية حيث تكون كلمات المرور:

- At least eight (8) characters
- ما لا يقل عن ثمانية (8) أحرف

- Not based on anything somebody else could easily guess or obtain using person related information (e.g., names, telephone numbers, dates of birth, etc.)
- لا تستند إلى أي شيء يمكن لشخص آخر تخمينه أو الحصول عليه بسهولة باستخدام المعلومات المتعلقة بالشخص (مثل الأسماء وأرقام الهواتف وتواريخ الميلاد وما إلى ذلك)

- A combination of at least one character from each of the following four listed character types:
- مجموعة مكونة من حرف واحد على الأقل من كل نوع من أنواع الأحرف الأربعة المدرجة التالية:

- English uppercase letters (A-Z)
- English lowercase letters (a-z)
- Base 10 digits (0-9)
- Non-alphanumeric (such as ` ~! @ # $ % ^ & * ( ) _ + - = { } | \ : " ; ' < > ? , . / and space)

- أحرف انجليزية كبيرة (A-Z)
- أحرف انجليزية صغيرة (a-z)
- 10 أرقام أساسية (0-9)
- الرموز (مثل ` ~! @ # $٪ ^ & * ( ) _ + - = { } | \ :"؛ '<>؟،. / والمسافة)

3. Password Expiration

In order to prevent an attacker from making use of a password that may have been discovered, passwords are deemed temporary and must be changed regularly. IT department reserves the right to reset a user's password in the event a compromise is suspected or reported. The required frequency at which passwords must be changed varies based on the type of user, as defined below.

3. انتهاء صلاحية كلمة المرور

تعتبر كلمات المرور مؤقتة ويجب تغييرها بانتظام ، لمنع المهاجم من استخدام كلمة مرور قد تم اكتشافها.
يحتفظ قسم تكنولوجيا المعلومات بالحق في إعادة تعيين كلمة مرور المستخدم في حالة الاشتباه في وجود اختراق أو الإبلاغ عنه.
يختلف التكرار المطلوب لتغيير كلمات المرور بناءً على نوع المستخدم ، كما هو موضح أدناه.

- **Standard Users**

Standard users consist of faculty, staff and students that are not system administrators or processing credit card payments.

- Passwords must be changed every six (6) months.
- Passwords must not be reused for at least four (4) generations.
- Passwords must not be changed more than one (1) time per day.
- At least four (4) characters must be changed when new passwords are created.
- New passwords must comply with the password requirements defined in the previous section.

- **المستخدم الاعتيادي**

يتكون المستخدم الاعتيادي من أعضاء هيئة التدريس والموظفات والطلبة الذين ليسوا مسؤولي نظام أو يتعاملون مع بطاقات الائتمان.

- يجب تغيير كلمات المرور كل ستة (6) أشهر.
- يجب عدم إعادة استخدام كلمات المرور لمدة أربعة (4) أجيال على الأقل.
- يجب عدم تغيير كلمات المرور أكثر من مرة واحدة (1) في اليوم.
- يجب تغيير أربعة (4) أحرف على الأقل عند إنشاء كلمات مرور جديدة.
- يجب أن تتوافق كلمات المرور الجديدة مع متطلبات كلمة المرور المحددة في القسم السابق.

- **Privileged Users and Payment Card Industry Users**

Privileged users consist of users with elevated access to administer information systems and applications, most often in the Information Technologies Department. Payment Card Industry users responsible for processing payments in RAKAA. Such users have administrator access and these accounts are at a higher risk for compromise.

- Passwords must be changed every ninety (90) days.
- Passwords must not be reused for at least six (6) generations.
- Passwords must not be changed more than one (1) time per day.

- **المستخدمون المتميزون ومستخدموا بطاقات الدفع**

يتألف المستخدمون المتميزون من مستخدمين يتمتعون بوصول مرتفع لإدارة أنظمة وتطبيقات المعلومات ، وغالبًا ما يكون ذلك في قسم تكنولوجيا المعلومات. بالإضافة إلى مستخدمي بطاقات الدفع المسؤولين عن معالجة المدفوعات في المدرسة، حيث يتمتع هؤلاء المستخدمون بحق وصول المسؤول، وهذه الحسابات معرضة بدرجة أكبر لخطر الاختراق.

- يجب تغيير كلمات المرور كل تسعين (90) يومًا.
- يجب عدم إعادة استخدام كلمات المرور لمدة ستة (6) أجيال على الأقل.
- يجب عدم تغيير كلمات المرور أكثر من مرة واحدة (1) في اليوم.

- At least four (4) characters must be changed when new passwords are created.
- New passwords must comply with the password requirements defined in the previous section.

- يجب تغيير أربعة (4) أحرف على الأقل عند إنشاء كلمات مرور جديدة.
- يجب أن تتوافق كلمات المرور الجديدة مع متطلبات كلمة المرور المحددة في القسم السابق.

4. Account Lockout

In order to limit attempts at guessing passwords or compromising accounts, an account lockout policy is in effect for all systems. Account lockout thresholds and durations vary based on the type of user, as defined below.

- **Standard Users**

  Standard user accounts have the following lockout policy:
  - Accounts will lockout after eighteen (18) invalid password attempts in fifteen (15) minutes.
  - Accounts will remain locked for a duration of fifteen (15) minutes, unless the IT department is contacted, and the user's identity is verified in order for the account to be unlocked sooner.

- **Privileged Users and Payment Card Industry Users**

  Privileged and Payment Card Industry user accounts have the following lockout policy:
  - Accounts will lockout after twelve (12) invalid password attempts in fifteen (15) minutes.
  - Accounts will remain locked for a duration of fifteen (15) minutes, unless the IT department is contacted, and the user's identity is verified in order for the account to be unlocked sooner.

4. تأمين الحساب

للحد من محاولات تخمين كلمات المرور أو اختراق الحسابات ، يتم تطبيق سياسة تأمين الحساب لجميع الأنظمة. تختلف حدود ومدة تأمين الحساب بناءً على نوع المستخدم ، كما هو محدد أدناه:

- **المستخدم الاعتيادي**

  حسابات المستخدم الاعتيادي لديها سياسة التأمين التالية:
  - سيتم إغلاق الحسابات بعد ثمانية عشر (18) محاولة غير صالحة لإدخال كلمة المرور خلال خمسة عشر (15) دقيقة.
  - ستظل الحسابات مقفلة لمدة خمسة عشر (15) دقيقة ، ما لم يتم الاتصال بقسم تكنولوجيا المعلومات ، ويتم التحقق من هوية المستخدم حتى يتم إلغاء قفل الحساب في وقت أقرب.

- **المستخدمون المتميزون ومستخدمو بطاقات الدفع**

  تتبع حسابات المستخدمين المتميزة وبطاقات الدفع سياسة الإغلاق التالية:
  - سيتم إغلاق الحسابات بعد اثني عشر (12) محاولة غير صالحة لإدخال كلمة المرور خلال خمسة عشر (15) دقيقة.
  - ستظل الحسابات مقفلة لمدة خمسة عشر (15) دقيقة ، ما لم يتم الاتصال بقسم تكنولوجيا المعلومات والتحقق من هوية المستخدم حتى يتم فتح الحساب في وقت أقرب.

5. Mobile Devices

Mobile devices accessing or storing data, such as smartphones and tablets, shall be tagged and managed by the mobile device management (MDM) platform.

The following minimum password policy is in effect for all mobile devices, where passwords are:

- At least six (6) complex digits

5. الأجهزة المحمولة

يجب وضع علامات على الأجهزة المحمولة التي تصل إلى البيانات أو تخزنها ، مثل الهواتف الذكية والأجهزة اللوحية ، وإدارتها بواسطة نظام إدارة الأجهزة المحمولة (MDM).

سياسة الحد الأدنى لكلمة المرور التالية سارية لجميع الأجهزة المحمولة ، حيث تكون كلمات المرور:

- ما لا يقل عن ستة (6) أرقام معقدة

- No repeating or sequential digits (e.g., 111111, 123456, or 101010)
- Changed every six (6) months.

Fingerprint readers on mobile devices may be used to unlock the device, but a compliant password must still be established.

- لا توجد أرقام مكررة أو متسلسلة (على سبيل المثال ، 111111 أو 123456 أو 101010)
- يتم التغيير كل ستة (6) أشهر.

يمكن استخدام قارئات بصمات الأصابع على الأجهزة المحمولة لإلغاء قفل الجهاز، ولكن لا يزال يتعين إنشاء كلمة مرور متوافقة.

6. Recommendations for Creating Compliant Passwords

In order to create a password that is compliant with the parameters specified in this policy, use one of the three methods below.

- **Use a Passphrase**

A passphrase is similar to a password, but it is generally longer and contains a sequence of words or other text to make the passphrase more memorable. A longer passphrase that is combined with a variety of character types is exponentially harder to breach than a shorter password.

- **Use an Acronym**

An acronym can be used to constitute a strong and compliant password by taking the first letter of each word in a phrase (including punctuation) to form the password.

- **Use a Secret Code**

A secret code can be used in conjunction with the previous methods simply by substituting letters for other numbers or symbols. Combining these methods will make it easy to incorporate the four-character types in order to meet the password complexity requirements.

6. توصيات لإنشاء كلمات مرور متوافقة

لإنشاء كلمة مرور متوافقة مع الشروط المحددة في هذه السياسة ، استخدم إحدى الطرق الثلاث أدناه.

- **استخدم عبارة المرور**

تشبه عبارة المرور كلمة المرور ، ولكنها عمومًا أطول وتحتوي على سلسلة من الكلمات أو نص آخر لجعل عبارة المرور أكثر قابلية للتذكر. يعد اختراق عبارة المرور الأطول التي يتم دمجها مع مجموعة متنوعة من أنواع الأحرف أكثر صعوبة من اختراق كلمة المرور الأقصر.

- **استخدم اختصارًا**

يمكن استخدام اختصار لتكوين كلمة مرور قوية ومتوافقة عن طريق أخذ الحرف الأول من كل كلمة في عبارة (بما في ذلك علامات الترقيم) لتشكيل كلمة المرور.

- **استخدم الرمز السري**

يمكن استخدام الرمز السري مع الطرق السابقة ببساطة عن طريق استبدال الأحرف بأرقام أو رموز أخرى. سيؤدي الجمع بين هذه الطرق إلى تسهيل دمج الأنواع المكونة من أربعة أحرف من أجل تلبية متطلبات كلمة المرور المعقدة.

7. Password Reset Options

Various options are available to assist users with changing a forgotten or expired password. The preferred and fastest method is through the use of the password management system. Personalized security questions must be setup in order to use this system to reset your password.

- **Password Self Service**

If you have forgotten your password, you will be required to validate your identity by answering security questions.

- In Person

Reset your password through the IT department.

7. خيارات إعادة تعيين كلمة المرور

تتوفر خيارات مختلفة لمساعدة المستخدمين في تغيير كلمة المرور المنسية أو منتهية الصلاحية. الطريقة المفضلة والأسرع هي من خلال استخدام نظام إدارة كلمات المرور. يجب إعداد أسئلة الأمان المخصصة من أجل استخدام هذا النظام لإعادة تعيين كلمة المرور الخاصة بك.

- **خدمة كلمة المرور الذاتية**

إذا كنت قد نسيت كلمة المرور الخاصة بك ، فسيُطلب منك التحقق من هويتك من خلال الإجابة على أسئلة الأمان.

- شخصيا

أعد تعيين كلمة المرور الخاصة بك من خلال قسم تكنولوجيا المعلومات.

RAK AA
RAS AL KHAIMAH AMERICAN ACADEMY
أكاديمية رأس الخيمة الأمريكية

AGREEMENT FORM

By signing this form and turning it in to IT department you agree to the terms of the Password Policy and Guidelines.

All fields are required.

Name: _____

Signature: _____

Date: _____

نموذج الاتفاق

من خلال التوقيع على هذا النموذج وتسليمه إلى قسم تكنولوجيا المعلومات ، فإنك توافق على شروط سياسة وإرشادات كلمة المرور.

جميع الحقول مطلوبة.

الاسم: _____

التوقيع: _____

التاريخ: _____