سياسة حماية كلمات المرور

تعريف كلمة المرور أو كلمة السر (Password) :

هي عبارة عن آلية أمان أساسية وعادةً ما يتم استخدامها للوصول إلى نظام أو تطبيق، أو خدمة خاصة ، ويتم استخدامها في معظم الحالات مع اسم مستخدم(Username) ، وتعتبر كلمة المرور من أكثر إجراءات المستخدمة في جميع الأجهزة الرقمية والمحوسبة للتحكم في الوصول، وعادةً ما يتم إنشاء كلمة المرور من قبل المستخدم نفسه في معظم التطبيقات والخدمات، وتكون منفصلة ومختلفة لكل نظام أو خدمة.

الغرض من سياسة حماية كلمة المرور :

- تحديد سياسات وإجراءات كلمة المرور لتقديم أفضل مستوى للخدمة مع أعلى درجات الحماية والخصوصية للمستخدمين.
- وضع معيار لإنشاء كلمات مرور قوية وحماية كلمات المرور هذه وتكرار التغيير.
- التعريف بكيفية استخدامها لكل فرد داخل المجتمع المدرسي.

النطاق :

تسري هذه السياسة على :

- ✓ الموظفين
- ✓ الطلاب
- ✓ الضيوف
- ✓ وجميع من يستخدم كافة الأجهزة وملحقاتها والخدمات المرتبطة بها والأنظمة و شبكات وبرامج المدرسة.

أنواع السياسات المتبعة لكلمات المرور:

1. سياسة كلمة المرور العامة:

- تتبع المدرسة سياسة لكلمات المرور لحماية أنظمتها. هناك مسؤوليات إدارية واضحة بالإضافة إلى سياسة معممة بشكل واضح.

- يحصل جميع المستخدمين على وصول ملائم ومحمي بكلمة مرور من أجل الوصول إلى أنظمة المدرسة كما أنهم تلقوا تدريبا ملائما بهذا الخصوص.
- تطبق المصادقة الآمنة على المستخدمين من الموظفين الذين يمتلكون صلاحية الوصول إلى البيانات السرية أو الحساسة بما في ذلك إمكانية الوصول إلى أنظمة المدرسة من خارجها.
- تُطبق كلمة مرور آمنة على أجهزة المستخدمين من الموظفين الذين يمتلكون صلاحية الوصول إلى البيانات السرية أو الحساسة ويشمل ذلك الأجهزة المدرسية في جميع مختبرات المدرسة ومكاتبها.
- تطبق إجراءات روتينية لحل أي اشكالات تتعلق بكلمات المرور.
- تطبق خاصية التحقق بخطوتين أو ما يماثلها عند الوصول إلى أنظمة البيانات السرية أو الحساسة مثل أنظمة إدارة المعلومات ، الطلبة ، الموظفين ... .
- تطبق قواعد روتينية لتغيير كلمات المرور بشكل دوري بالإضافة إلى فرض استخدام كلمات مرور قوية عند تجديدها.
- قد يخضع الطلاب أو أعضاء الهيئة التدريسية أو الموظفون الذين يثبت انتهاكهم لهذه السياسة لإجراءات تأديبية تصل إلى إنهاء التوظيف و / أو التعليق و / أو الطرد .
- فرض كلمة مرورية قوية ولا تتضمن في تركيبها الكلمات التي يسهل على الآخرين التكهن بها وفق التالي:
  - ✓ يجب استخدام توليفة من الأحرف الكبيرة والصغيرة، مع أرقام، ورموز أو علامات الترقيم قدرالإمكان عند اختياركلمة المرور. (ويفضل أن تكون ذات دلالة خاصة للمستخدم لتجنب نسيانها)
  - ✓ لا يجب استخدام كلمات سر رائجة والتي يمكن التكهن بها بسهولة، كالأسماء وتاريخ الميلاد أوارقام الهواتف
  - ✓ يجب ألا يقل عدد رموز كلمة السر المرور من 8 رمزا
  - ✓ لا يجب استعمال اسم المستخدم في كلمة السر
  - ✓ لا يجب استخدام أرقام أو حروف متكررة مثل (3333 أو(AAAA).
  - ✓ يجب تغيير كلمة السر بشكل دوري لزيادة الأمان .
  - ✓ يفضل عدم استخدام كلمة السر نفسها لجميع الحسابات
  - ✓ لا تكتب كلمات المرور وتخزنها في أي مكان في مكتبك.
  - ✓ لا تخزن كلمات المرور في ملف على أي نظام كمبيوتر غير مشفر.

2. سياسة كلمات المرور بالنسبة لأجهزة الحاسوب ومواقع التواصل الاجتماعي المدرسة :

- جميع أجهزة التكنولوجيا بالمدرسة محمية بكلمة مرور قوية ويتم تغييرها بشكل دوري .
- يتم حفظ كلمات المرور في ملف خاص.

3. سياسة كلمة المرور بالنسبة للموظفين :

منصات وبرامج المدرسة (Paradigm – MS TEAMS)

- تتيح مدرسة الشارقة الدولية الحق للموظف بتغيير كلمة المرور على جميع منصات وبرامج المدرسة ماعدا MS TEAMS.
- في حال نسيانها أو ضياعها يمكن للموظف إعادة تعيينها أو الاستعانة بقسم الدعم الفني للمساعدة.
- بالنسبة لل MS TEAMS يمكن للموظف الاستعانة بقسم الدعم الفني للمساعدة.
- لا تحتفظ المدرسة بكلمات السر للموظفين بل تقوم بتغييرها في حال نسيانها من قبل الموظف.
- يحق فقط للمعلمتين من الدعم الفني مساعدة المعلم في استعادة كلمات السر لبرامج ومنصات المدرسة (أ. عفاف أبوستة للقسم البريطاني – و أ. أميرة لولو للقسم الوزاري)
- إذا اشتبه في اختراق حساب أو كلمة مرور ، فيتم أبلاغ منسق السلامة الإلكترونية بالحادث ويجب تغيير جميع كلمات المرور وتطبيق المصادقة الآمنة على حساب المعلم.

4. سياسة كلمة المرور بالنسبة للطلاب :

- تحتفظ المدرسة بحق تغيير كلمات المرور للطالب علي منصتي MS Teams أو PARADIGM .
- يتم تغيير كلمات المرور للطلاب اذا اقتضت الحاجة.
- في حال نسيان الطالب لحسابه أو لكلمة المرور الخاصة بإحدى المنصتين أو كلاهما يجب على الطالب التواصل مع قسم الدعم الفني بأحد لطرق التالية والمنتشرة علي مواقع التواصل وعلى منصة TEAMS :
  - الاتصال أو ارسال واتس اب على الرقم 0509501106 للقسم البريطاني والرقم 0569920110 للقسم الوزاري من رقم ولي الأمر المسجل لدي شؤون الطلبة .
  - الاتصال بالمدرسة والتي تقوم بتحويل المشكلة لقسم الدعم الفني.
- يحق فقط لفريق الدعم الفني مساعدة الطالب في استعادة كلمات السر لبرامج ومنصات المدرسة .
- لا تحتفظ المدرسة بسجل لكلمات المرور الخاصة بالطالب ، انما تقوم بتغييرها في حال طلب ذلك.
- إذا اشتبه في اختراق حساب أو كلمة مرور ، يتم إبلاغ منسق السلامة الإلكترونية بالحادث .

5. سياسة كلمة المرور بالنسبة WIFI:

- موظفين : تتيح مدرسة الشارقة الدولية للموظف استخدام شبكة المدرسة (WIFI) وربط جهاز واحد عليها بواسطة MAC Address.
- طلاب : تتيح مدرسة الشارقة الدولية للطالب استخدام شبكة المدرسة (WIFI) وربط جهاز واحد عليها بواسطة MAC Address.
- زوار : تتيح مدرسة الشارقة الدولية للضيوف استخدام شبكة المدرسة (WIFI) وربط الجهاز علي الشبكة بواسطة OTP Vouchers (1 or 8 hours)

6. تأمين كلمات المرور:

- يجب تخزين كلمة المرور بطريقة آمنة تضمن عدم كشفها.
- الحفاظ على سرية كلمات المرور فيجب عدم مشاركة أو كشف كلمة المرور مع أي شخص لأي سبب من الأسباب.
- يجب تغيير كلمات المرور إذا ظهر أي مؤشر على احتمال اختراق النظام أو اختراق لكلمة المرور.
- لا تخزن كلمات المرور في ملف على نظام كمبيوتر مدرسي أو أجهزة محمولة (هاتف، كمبيوتر لوحي) تابعة للمدرسة.
- يفضل عدم استخدم ميزة "تذكر كلمة المرور" للتطبيقات.
- يتطلب تغيير كلمات المرور بشكل دوري لكل من الأجهزة والبرامج المدرسية والموظفين العاملين بالمدرسة.
- قسم دعم فني مختص بعملية تأمين كلمات المرور بحيث يقوم بتحديث الكلمات بالإضافة لحرصهم الشديد على المحافظة على سرية كلمات المرور وإرسالها بشكل خاص سواء للطلاب او الكادر التعليمي.

7. التوعية بأهمية كلمات المرور:

- نشر ثقافة الأمن والسلامة الرقمية.
- عقد دورات للطلاب وأولياء الأمور والعاملين بالمدرسة لشرح الطريقة الأمثل لاختيار كلمات المرورPassword .
- التوعية المستمرة لكل من المعلمين وأولياء الأمور والطلاب .
- تثقيف أولياء الأمور بأهمية محافظة الطالب على سرية حساب المستخدم و كلمة المرور الخاصة به وتوعيتهم بذلك جيدا.
- يجب علي الطالب / أولياء الأمور إبلاغ الإدارة اذا حدث اختراق لحساب الطالب أو قام أحدهم باستخدام حساب الطالب.
- التناول المستمر أثناء حصص التصميم و التكنولوجيا وICT عن كيفية حماية كلمة المرور وعدم مشاركتها مع شخص آخر.
- تعرض بشكل دوري قبل بداية معظم الحصص الفيديوهات المسجلة عن كيفية حماية كلمة المرور وعدم مشاركتها مع شخص آخر للتوعية.
- المشاركة الطلابية لتوعية زملائهم عبر تسجيل فيديوهات عن كيفية حماية كلمة المرور وعدم مشاركتها مع شخص آخر وهي منتشرة على منصتي TEAMS , TELEGRAM
- عقد ورش تدريبية تحت عنوان حماية كلمة المرور والحسابات الشخصية لكل من المعلمين وأولياء الأمور.

إيقاف حساب مدرسي أوتعطيله مؤقتا:

يتم حذف جميع حسابات و كلمات المرور التي لم تعد مطلوبة أو تعطيلها لعدة أسباب منها على سبيل المثال لا الحصر :

- ❖ إنهاء عقد موظف
- ❖ ترك طالب الدراسة.
- ❖ مخالفة موظف أو طالب لسياسات المدرسة أو لائحة السلوك.

الاجراء :

- يتم إبلاغ مسؤولة السلامة الرقمية في حال ترك موظف أو طالب المدرسة .
- تقوم مسؤولة السلامة الالكترونية بعد ذلك بحذف حساب المستخدم أو تعليقه.
- سيتحقق فرد ثان من هذا القسم للتأكد من حذف حساب المستخدم أو تعليقه.

مديرة المدرسة :

سوسن عبد الفتاح

Password Policy

Definition:

It is a basic security mechanism and is usually used to access a system, application, or special service, and it is used in most cases with a username, and the password is one of the most common procedures used in all digital and computerized devices to control access, usually the password is created by the same user in most applications and services, and it is separate and different for each system or service.

The purpose of the password protection policy:

- Defining password policies and procedures to provide the best level of service with the highest degree of protection and privacy for users.
- Establishing a standard for creating strong passwords, protecting these passwords and changing frequency.
- Defining how to use it for everyone within the school community.

To whom this policy applies:

This policy applies to:

- employees
- students
- guests

And all those who use school devices, and associated services, systems, networks and school platforms.

Types of passwords policies:

1. General Password Policy:

•The school follows a password policy to protect its systems. There are clear management responsibilities as well as a clearly generalized policy.

•All users receive adequate, password-protected access to school systems and have received appropriate training in this regard.

•Secure authentication applies to employee users who have access to confidential or sensitive data.

•A secure password is applied to all devices of employees who have access to confidential or sensitive data, and this includes school devices in all school laboratories and offices.

•Routines are applied to resolve any password issues.

•The two-step verification feature or something similar is applied when accessing confidential or sensitive data systems such as information management systems, students, employees...

•Apply routine rules to change passwords periodically in addition to imposing the use of strong passwords when renewing them.

•Students, faculty, or staff found to have violated this policy may be subject to disciplinary measures up to termination of employment, suspension and / or expulsion.

•Imposing a strong password that does not include in its composition the words that are easy for others to guess according to the following:

- ✓ A combination of uppercase and lowercase letters, with numbers, symbols or punctuation marks should be used whenever possible when choosing a password. (It is preferred that it be of special significance to the user to avoid forgetting it)
- ✓ Do not use popular passwords that can be easily guessed, such as names, date of birth or phone numbers
- ✓ The password must be at least 8 characters long
- ✓ The username should not be used in the password
- ✓ Do not use repeated numbers or letters such as (3333 or AAAA).
- ✓ The password must be changed periodically to increase security.
- ✓ It is preferable not to use the same password for all accounts
- ✓ Do not write passwords and store them anywhere in your office.
- ✓ Do not store passwords in a file on any unencrypted computer system.

2. Password policy for school computers and social media sites:

•All school technology devices are protected with a strong password and it is changed periodically.

Passwords are saved in a special file.

3.Password policy for employees:

School platforms and programs (Paradigm - MS TEAMS)

•Sharjah International School grants the right of the employee to change the password on all school platforms and programs except for MS TEAMS.

•In the event of a forgetfulness or loss, the employee can reassign it or seek help from the technical support department.

•For MS TEAMS, the employee can seek help from the Technical Support Department.

•The school does not keep employee passwords, but rather changes them in case the employee forgot them.

•Only the two technical support teachers have the right to assist the teacher in recovering passwords for the school's programs and platforms (A. Afaf Abusta for the British section - and A. Amira Lulu for the ministerial department)

•If an account or password is suspected to have been compromised, the incident is reported to the Cyber Safety Coordinator and all passwords must be changed and secure authentication applied to the teacher's account.

4. Password policy for students:

•The school reserves the right to change the student's passwords on the MS Teams or PARADIGM platforms.

•Passwords are changed to students if needed.

•In the event that the student forgets his account or the password for one or both of the two platforms, the student must contact the Technical Support Department in one of the following ways, which are spread on the communication sites and on the TEAMS platform:

o Calling or sending WhatsApp to the number 0509501106 of the British Department and the number 0569920110 of the Ministerial Department from the number of the guardian registered with Student Affairs.

o Contact the school, which refers the problem to the technical support department.

•Only the technical support team has the right to assist the student in recovering passwords for the school's programs and platforms.

•The school does not keep a record of the student's passwords, but rather changes them if requested.

•If it is suspected that an account or password has been compromised, the cyber safety coordinator shall be informed of the incident.

5. WIFI Password Policy:

•Staff: Sharjah International School allows the employee to use the school's network (WIFI) and connect one device to it via MAC Address.

Students: Sharjah International School allows students to use the school's network (WIFI) and connect one device to it via MAC Address.

Visitors: Sharjah International School allows guests to use the school's network (WIFI) and connect the device to the network via OTP Vouchers (1 or 8 hours)

6. Passwords securing:

•The password must be stored in a secure way to ensure that it is not exposed.

•Maintain a confidentiality

Passwords You should not share or disclose your password with anyone for any reason.

•Passwords must be changed if there is any indication that the system or the password may be hacked.

•Do not store passwords in a file on a school computer system or mobile devices (phone, tablet) belonging to the school.

•It is preferred not to use the "remember the password" feature of the applications.

•It requires changing the passwords periodically for each of the school devices and programs and the school staff.

•A technical support department specialized in the process of securing passwords so that it updates the words in addition to their keenness to maintain the confidentiality of passwords and send them in particular, whether to students or educational staff.

7. Awareness of the importance of passwords:

Disseminating a culture of digital safety and security.

•Holding courses for students, parents and school staff to explain the best way to choose passwords. Password

•Ongoing awareness of teachers, parents and students.

•Educating parents about the importance of the student's preservation of the confidentiality of his user account and password, and making them aware of that well.

•The student / parents must inform the administration if the student's account is hacked or one of them uses the student's account.

•Continuous discussion during the design, technology and ICT sessions on how to protect the password and not share it with another person.

•Recorded videos are shown periodically before the start of most lessons on how to protect the password and not share it with another person to raise awareness.

•Student participation to educate their colleagues by recording videos on how to protect the password and not to share it with another person. It is spread on the TEAMS and TELEGRAM platforms.

•Holding training workshops under the title of password protection and personal accounts for both teachers and parents.

8. Suspending or temporarily disabling a school account:

All accounts and passwords that are no longer required are deleted or disabled for a number of reasons, including but not limited to:

 Termination of an employee's contract

 Student dropped out.

An employee or student violating school policies or behavior regulations.

Action:

•The digital safety officer is informed in the event that an employee or student leaves the school.

•The electronic safety official then deletes or suspends the user's account.

•A second individual will check this section to ensure that the user's account has been deleted or suspended.

School Principal