وزارة التعليم
Ministry of Education

الإدارة العامة لأمن المعلومات

INFORMATION SECURITY GENERAL DIRECTORATE

سياسة الاستخدام المقبول للموارد والخدمات التقنية

ACCEPTABLE USE POLICY OF INFORMATION ASSETS

اعتمد هذه السياسة معالي وزير التعليم
د. أحمد بن محمد العيسى
في
2 ربيع الأول 1438 هـ

النسخة
6.3
Version

Introduction

IT enables the Ministry of Education mission to provide the best educational services, through IT reliable technology, aimed at supporting Ministry services that are used by wide range of users.

This policy was developed to protect the resources and technical services provided by the IT, and to maintain the confidentiality, integrity, and privacy of the data. Also, to ensure that sources of information are available when needed and to emphasize the users understanding of their responsibilities toward protecting the information assets.

Policy

1. Email

- Email is a formal communication. Employees should maintain suitable and professional langue in emails.
- Only official email should be used for all official and business related communications.
- Creating or sending unsolicited, unwanted, or inappropriate messages and chain letters is prohibited.
- Opening unknown or suspicious attachments or clicking on links in emails from unknown senders is prohibited.
- Using/Sharing the Ministry's email for unofficial purposes (mailing lists, blogs, forums, and Internet sites) is prohibited.
- Using email accounts such as Hotmail, Google, etc. for exchanging official information is prohibited.

2. Network & Internet

- Internet is provided to staff for business use only, it shall not be used for personal benefit.
- Viewing or downloading inappropriate material (offensive, pornographic materials, jokes, or any other comments/material that would be expected to offend someone for their physical or mental

مقدمة

يعنى قطاع تقنية المعلومات بتمكين وزارة التعليم من تقديم أفضل الخدمات التعليمية من خلال تقنية موثوقة ذات كفاءة وفاعليه، لمساندة شريحة واسعة من المستفيدين من خدمات الوزارة.

وحرصا على توفير خدمات الكترونية آمنة متماشية مع التنظيمات والتوجيهات الحكومية الصادرة في هذا المجال تم تطوير هذه السياسة بهدف حماية الموارد والخدمات التقنية التي يقدمها قطاع تقنية المعلومات، والمحافظة على سرية وسلامة وخصوصية البيانات، وعلى أن تكون مصادر المعلومات متاحة عند الحاجة إليها، وللتأكيد على أهمية فهم المستخدمين لمسؤولياتهم تجاه حمايتها.

السياسة

1. البريد الالكتروني

- البريد الإلكتروني يعتبر وسيلة تواصل رسمية، ويجب على مستخدميه مراعاة ذلك عند اختيار لغة التخاطب عبر البريد الإلكتروني.
- يجب استخدام البريد الالكتروني الرسمي فقط للمعاملات الرسمية وللأغراض المتعلقة بالعمل.
- يحظر استخدام البريد لإرسال أو إنشاء رسائل غير مرغوب فيها أو غير لائقة أو غير شرعية.
- يحظر فتح المرفقات غير المعروفة أو المشبوهة أو النقر على الروابط المدرجة في رسائل البريد الالكتروني المرسلة من قبل جهات غير معروفة أو غير موثوقة.
- يحظر استخدام عنوان البريد الالكتروني الخاص بالوزارة لأغراض غير رسمية (قوائم البريد، المدونات، المنتديات، ومواقع الانترنت).
- يحظر استخدام حسابات البريد الالكتروني المجاني في المعاملات الرسمية أو الأغراض المتعلقة بالعمل (مثل قوقل أو ياهو أو هوتميل أو غيرها).

2. الشبكة والانترنت

- خدمة الإنترنت المقدمة من قبل الوزارة هي لأغراض العمل فقط ولا يجب أن تستخدم لأي أغراض شخصية.
- يحظر مشاهدة أو تنزيل محتوى غير ملائم (مواد مسيئة، صور أو محتويات إباحية، نكات أو أي تعليقات أخرى قد تؤدي إلى الإساءة إلى أي شخص على أساس الإعاقة الجسدية

disability, age, religion, marital status, national origin and/or race) is prohibited.

- Using the Network and Internet to attempt unauthorized access to other computers, information or services is prohibited.
- Downloading or copying of copyrighted material, including software, books, articles, and photographs, which are not licensed for use by MOE is prohibited.
- Only the internet access provided by MOE in its work sites can be used; Using any other sources of Internet such as Modems, 3G/ 4G USB modems ... etc., is prohibited.
- Undertaking any activity that may introduce viruses or other malicious software on MOE's network is prohibited.
- Representing the Ministry in the social networks or sending news on its behalf is prohibited without proper authorization.

3. Desktops/Laptops and Storage Media

- Desktops/Laptops must not be left unattended without screen lock and using cable locks for Laptops is preferred.
- Desktops/Laptops and storage media must be physically secured at all times (airport, car, home, office etc.).
- Staff must not attempt to install/uninstall any software or hardware without proper authorization from IT.
- Staff must not attempt to install or use unlicensed software. It is also prohibited to share or distribute unlicensed software using ministry computers or storage media.
- Modifications to security settings (password and lockout policies, security system, antivirus etc.) are prohibited.
- Desktops/Laptops and storage media containing confidential or secret information must be authorized by IT (or IT management in education directorates) prior to moving it out of MOE premises.

أو العقلية، أو بسبب العمر، أو الدين، أو الحالة الاجتماعية، أو العِرق).

- يحظر استخدام الشبكة والانترنت لمحاولة الدخول غير المصرح إلى أجهزة الكمبيوتر أو المعلومات أو الخدمات.
- يحظر تنزيل أو نسخ مواد محمية بموجب حقوق الملكية الفكرية بما في ذلك البرمجيات، والكتب، والمقالات، والصور التي لا تكون مرخصة لوزارة التعليم.
- يحظر استخدام أي مصدر للإنترنت (مثل المودم الثابت أو مودم الجيل الرابع أو الثالث أو ما شابهها) غير ما يتم توفيره من قبل الوزارة في مواقع العمل.
- يحظر القيام بأية أنشطة من الممكن أن تعرض شبكة وزارة التعليم إلى مخاطر الفيروسات أو البرامج الخبيثة.
- يحظر استخدام شبكات التواصل الاجتماعي باسم الوزارة أو نشر أخبار تتعلق بها إلا عن طريق الجهات المصرح لها بذلك.

3. الحواسيب المكتبية والمحمولة ووسائط تخزين البيانات

- يحظر ترك الأجهزة دون قفل الشاشة كما يفضل استخدام كابل الحماية للأجهزة المحمولة.
- يجب ضمان حماية الأجهزة ووسائط التخزين في جميع الأوقات والمحافظة عليها في أي مكان كالمطار أو السيارة أو المنزل أو المكتب.
- يحظر على كل موظف أن يقوم بمحاولة تحميل أو إزالة أية برمجيات أو تركيب أية قطع دون الحصول على الموافقات اللازمة من تقنية المعلومات.
- يمنع تركيب أو استخدام البرمجيات الغير مرخصة باسم الوزارة على الأجهزة، كما يمنع تخزين وتبادل البرمجيات على وساط التخزين والأجهزة في حال عدم توفير الوزارة للرخص اللازمة لتلك البرمجيات.
- يحظر إجراء أية تعديلات على إعدادات الأمن (مثل اعدادات كلمة السر، قفل الشاشة، الجدار الناري، برامج مكافحة الفيروسات).
- يجب الحصول على موافقة تقنية المعلومات (أو من يقوم مقامهم في إدارات التعليم) عند نقل الأجهزة ووسائط التخزين التي تحتوي على معلومات تخص العمل قبل نقلها إلى خارج مواقع الوزارة.

- Lost or stolen laptops or storage media must be immediately reported to the IT or authorized IT management in education directorates.
- Eating and drinking while working on devices is prohibited.
- Laptops and storage media devices must not be checked as luggage at the airport, but instead they must be carried onboard as hand luggage.
- Using personal devices (laptops, USB memory stick, smart phones etc.) for storing or processing MOE's information is prohibited.

4. Printer & Fax Machines

- Printing facility must be used for official purposes only.
- Confidential and secret information must not be sent through fax.
- Information classified as For Official Use Only must be labeled when sending it through fax.
- For Official Use Only, Confidential and Secret information must not be left unattended on shared printers.

5. User Password Management

- Default passwords must be changed when they are first used.
- Password must be complex and hard-to-guess
- Password must be a combination of numbers and characters, and adding special characters is preferred.
- Passwords must be at least eight (8) characters in length.
- Password shall be changed periodically, and it is preferable to use the password only once.
- Password shall not be disclosed or shared with others.

- يجب إبلاغ تقنية المعلومات (أو من يقوم مقامهم في إدارات التعليم) فور فقدان أو سرقة الأجهزة أو وسائط التخزين.
- يحظر تناول المأكولات أو المشروبات أثناء العمل على الأجهزة.
- يحظر شحن الأجهزة المحمولة ووسائط التخزين مع حقائب الأمتعة في حالة السفر، ويجب حملها مع الامتعة المحمولة باليد.
- يحظر استخدام الأجهزة الخاصة (مثل اجهزة التخزين المتنقلة والحاسب المحمول وأجهزة الاتصالات الذكية وغيرها) لتخزين أو معالجة معلومات تخص الوزارة.

4. الطابعات والفاكسات

- يجب استخدام الطابعات للأغراض الرسمية فقط.
- لا يجوز إرسال معلومات سرية عبر الفاكس.
- يجب وضع إشارة خاصة على المعلومات التي تصنف على أنها "للاستخدام الرسمي فقط" عند إرسالها بواسطة الفاكس.
- يجب عدم ترك الوثائق التي تتضمن معلومات سرية أو ذات الخصوصية على الطابعات المشتركة.

5. إدارة كلمة السر للمستخدم

- يجب تغيير كلمة السر عند أول استعمال لها.
- يجب أن يجتهد المستخدم في اختيار كلمة سر صعبة التخمين.
- يجب أن تكون كلمة السر خليط بين الأحرف والأرقام، ويفضل كذلك استعمال الرموز الخاصة ما أمكن ذلك.
- يجب ألا يقل طول كلمة السر عن ثماني (8) خانات على الأقل.
- يجب تغيير كلمة السر بشكل دوري، ويفضل ألا يعاد استخدام كلمة السر أكثر من مرة.
- يجب المحافظة على كلمة السر وعدم نشرها او مشاركتها مع الآخرين.

6. Clear desk and clear screen policy

- Desks and working areas must be cleared of papers and removable computer storage media when not in use whether during or outside normal working hours.
- Unattended PCs or terminals must be locked by a suitable mechanism during the working day (password-protected screensaver, key lock, or token lock) and must be logged off completely at the end of the working day.

7. Voicemail

- Staff must ensure their recorded messages don't contain sensitive information.
- The owner of a voicemail box must regularly check incoming messages and delete messages already listened to as soon as possible.

8. Publicly available information

Formal authorization from General Directorate of public relations and Media Affairs (or authorized representative in Educational Directorate) must be obtained before any information is made publicly available in order to ensure accuracy and compliance with IT's security standards.

Transferring of MOE's data/information to unauthorized parties or leaking by any means is prohibited.

Acknowledgement

By using MOE's assets and services, I understand and will abide by the above Policy. I further understand that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges will be revoked, and/or appropriate legal action will be taken. I further understand that any violation of this policy shall be reported to IT.

For any queries or comments, please contact us on e-mail **security@moe.gov.sa**

6. سياسة المكتب النظيف والشاشة الخالية

- يجب أن تكون المكاتب وأماكن العمل خالية من الأوراق ومن وسائط التخزين المتنقلة في حال عدم الحاجة لها خلال ساعات العمل المعتادة أو خارجها.
- يجب قفل أجهزة الكمبيوتر في حالة عدم التواجد من خلال آلية ملائمة خلال أيام العمل (مثل كلمة سر لحماية الشاشة) ويجب الخروج من الأنظمة كليا في نهاية العمل.

7. البريد الصوتي

- عند الحاجة لترك رسالة صوتيه يجب التأكد من عدم احتوائها على معلومات سريه.
- يجب على صاحب صندوق البريد الصوتي أن يقوم بانتظام بتفقد الرسائل الواردة وحذف الرسائل التي تم سماعها بأسرع ما يمكن.

8. المعلومات المتاحة للجمهور

يجب الحصول على موافقة رسمية من الادارة العامة للعلاقات والاعلام (أو من يقوم مقامهم في إدارات التعليم) قبل نشر أية معلومات من اجل ضمان الدقة والالتزام بالمعايير الأمنية لتقنية المعلومات، كما يمنع نقل البيانات والمعلومات الخاصة بالوزارة لغير المصرح لهم، أو تسريبها بأي وسيلة.

الإقرار

استخدامي للموارد والخدمات التقنية يعني فهمي والتزامي بالسياسة أعلاه بشأن الاستخدام المقبول للموارد والخدمات التقنية، كما أؤكد فهمي أن أي انتهاك للوائح المذكورة غير مقبول وبعضها يمكن أن يشكل جريمة جنائية، ومخالفة قد يسبب إلغاء صلاحيات الدخول الممنوحة لي واتخاذ الإجراءات القانونية المناسبة بحقي، والتزم بتبليغ تقنية المعلومات عن أي مخالفات لهذه السياسة تصل الى علمي.

لأي استفسار أو ملاحظة يمكنكم التواصل معنا على البريد الإلكتروني **security@moe.gov.sa**