إدارة تقنية المعلومات

سياسة أمن المعلومات الرقمية

مدارس دلتا

الإدارة العامة – الرياض, حي المروج

اسم الإجراء	**سياسة أمن المعلومات الرقمية**			**رقم الإجراء**	**CS/IT/002**
تاريخ التفعيل	**2025/8/4**	**تاريخ آخر مراجعة**	**2025/8/4**	**رقم النسخة**	**1.1**
مالك الوثيقة	**طارق السوداني**			**رقم التواصل**	**204**
إشارة المشاركة	**أخضر**			**تصنيف الوثيقة**	**مشاركة داخل المدارس فقط**

تاريخ الإصدارات				
رقم الإصدار	تم اعتماده من قبل	تاريخ المراجعة	تفاصيل التغيير	التوقيع
1	تهاني الطويلي			
1.1	تهاني الطويلي	2025/8/4	تحديث في الإطار التنظيمي	

بروتوكول الإشارة الضوئية (TPL):

يستخدم هذا البروتوكول على نطاق واسع في العالم وهناك أربعة ألوان (إشارات ضوئية):

أحمر – شخصي وسري للمستلم فقط

المستلم لا يحق له مشاركة المصنف بالإشارة الحمراء مع أية فرد سواء من داخل أو خارج الجهة خارج النطاق المحدد للاستلام.

برتقالي – مشاركة محدودة

المستلم يمكنه مشاركة المعلومات في نفس الجهة مع الأشخاص المعنيين فقط, ومن يتطلب الأمر منه اتخاذ إجراء يخص المعلومة.

أخضر – مشاركة في نفس المجتمع

المستلم يمكنه مشاركة المعلومات مع آخرين في نفس الجهة أو جهة أخرى على علاقة معهم أو في نفس القطاع, ولا يسمح بتبادله أو نشرها من خلال القنوات العامة.

أبيض – غير محدود

إدارة تقنية المعلومات

محتويات الوثيقة

إدارة تقنية المعلومات

1- مقدمة

تلتزم مدارس دلتا بتوفير بيئة تعليمية آمنة إداريا وتكنولوجيا من خلال تطبيق سياسات وإجراءات أمنية متوافقة مع المعايير الدولية مثل ISO 27001, ITIL, COBIT, CIS Controls, والتي تهدف إلى ضمان سرية وسلامة توفر البيانات والمعلومات الرقمية وحماية البيانات الخاصة بالطلاب،المعلمين والإداريين, بما يحقق بيئة تعليمية آمنة و فعالة.

2- الأهداف العامة:

- ضمان حماية المعلومات والبيانات الرقمية من التهديدات الإلكترونية.
- توفير إطار تنظيمي يحدد ضوابط الأمن السيبراني داخل بيئة المدارس.
- تعزيز الوعي الأمني لدى جميع المستخدمين من طلاب، معلمين وإداريين.
- تطبيق أفضل الممارسات في إدارة المخاطر السيبرانية وفق المعايير الدولية.
- ضمان استمرارية الأعمال وتقليل المخاطر التشغيلية المتعلقة بأمن المعلومات.

3- نطاق السياسة:

تنطبق هذه السياسة على جميع العاملين في مدارس دلتا من معلمين وإداريين, بالإضافة لجميع الطلاب ومزودي الخدمات والمقاولين وجميع الأطراف الخارجية التي تتعامل مع الأصول المعلوماتية التابعة للمدارس, كما تشمل جميع منصات التعليم الإلكتروني المستخدمة.

4- تطبيق السياسة:

تتحمل الإدارة مسؤولية تطبيق هذه السياسة بالتعاون مع إدارة تقنية المعلومات لضمان الالتزام بالمعايير المعتمدة, كما يتم تقييم الالتزام بالسياسات من خلال مراجعات دورية, مع عمل تحديث للإجراءات متى اقتضت الحاجة وعند الضرورة, مع عمل اعتماد ونشر لتلك التحديثات.

5- الأحكام العامة:

- **السرية**: حماية البيانات من الوصول غير المصرح به.
- **السلامة**: ضمان عدم تعديل البيانات أو تلفها دون إذن.
- **التوفر**: التأكد من إتاحة البيانات للمستخدمين المخولين عند الحاجة.
- **الامتثال** : الالتزام بالقوانين واللوائح المحلية والدولية المتعلقة بأمن المعلومات.

---

6 - أمن التعلم الإلكتروني:

1- يتم استخدام منصات تعليمية معتمدة (كلاسيرا, ماجر وهيل, HMH) لضمان حماية البيانات التعليمية.
2- الالتزام بمعايير وأخلاقيات وآداب الدين الإسلامي الحنيف والأعراف والتقاليد الوطنية السائدة.
3- الالتزام بقوانين الدولة واللوائح المنظمة لوزارة التعليم.
4- يمنع استخدام برامج وأدوات تعليمية غير مرخصة.
5- تتم مراجعة وتأمين البيانات المتبادلة عبر منصات التعليم الإلكتروني.
6- احترام الآخرين بكل فئاتهم, وانتقاء لغة حوار مناسبة.
7- عدم نشر بيانات شخصية.
8- المعاملة الطيبة مع الآخرين وتقبل الآراء وعدم التنمر الإلكتروني بأي شخص.
9- المحتوى المنشور من قبل المستخدم يتحمل مسؤوليته أدبيا وقانونيا.
10- يحظر نشر مواد دعائية لأية جهة دون الحصول على موافقة رسمية من إدارة المدارس العليا.
11- يحظر قيام أية مستخدم بتنفيذ (متطلبات /مهام النظام) لمستخدم آخر, مهما كانت الأسباب مثال: حل المعلم لواجبات الطلاب أو قيام بنشاط تعليمي عوض عن الطالب, وسيتم تطبيق العقوبات حسب اللوائح المنصوص عليها.
12- حسابك في النظام هو حساب شخصي لا يحق بيعه أو تأجيره بغرض التربح أو مجانا، أو إرساله لشخص خارج المدرسة أو أشخاص تم إيقاف حساباتهم من مجتمع المدارس.
13- يتم تعطيل وحذف حسابات المعلمين والطلاب المنسحبين من قبل مدراء النظام.

7- أمن الحسابات وكلمات المرور:

- الحرص على سرية بيانات حسابات الدخول.
- يمنع مشاركة بيانات تسجيل الدخول مع أية شخص.
- إبلاغ قسم التقنية عن فقدان الحساب أو التأكد من دخول مريب عليه لاتخاذ الإجراءات اللازمة.
- الحرص على تسجيل الخروج من الحسابات في حال استخدام جهاز غير جهاز الخاص.
- الحذر من بعض السلوكيات التي قد تشكل خر على أمن وسرية المعلومات مثل:
  - الضغط على الروابط المجهولة لأنها من الممكن أن تكون روابط لتصيد المعلومات.
  - إرفاق روابط مجهولة أو غير قانونية داخل النظام.

- يتم تعطيل الحسابات الغير نشطة بعد إخلاء الطرف للموظفين, وبعد الانتقال لمدارس أخرى بالنسبة للطلاب.

8- استخدام الأنظمة والشبكات:

- يمنع تثبيت أو استخدام برامج غير معتمدة.
- تخضع جميع الأنشطة على الشبكة للمراقبة لضمان الامتثال.
- يمنع استخدام موارد المدرسة في أنشطة غير قانونية أو مخالفة للأخلاقيات.
- يحظر نشر أي محتوى ضار أو أكواد فيروسات بهدف الإضرار ببيئة الأنظمة، ويحق المقاضاة القانونية عند ثبوت ذلك.
- ينبغي الاطلاع على نظام مكافحة الجرائم المعلوماتية الصادر بقرار مجلس الوزراء رقم 79 وتاريخ 1428/3/7 وفهم العقوبات المتعلقة بالجرائم المعلوماتية أو المخالفات الرقمية .
- المستخدم مسؤول مسؤولية كاملة عن كل ما يتضمنه حساباته من مصادر ورسائل ونصوص وصور, ويحق اتخاذ العقوبات القانونية لمن يثبت مخالفته.
-

9- إدارة البيانات وحمايتها:

1- يتم تخزين البيانات الهامة في جهاز المدارس مع الاحتفاظ بنسخة منه على الدرايف الخاص بالمدارس.
2- يمنع مشاركة المعلومات الحساسة عبر الوسائل غير الآمنة.
3- يتم إجراء نسخ احتياطية دوري للملفات ورفعها على الدرايف الخاص .

10- حقوق الملكية:

- احترام قوانين وحقوق الملكية الفكرية والنسخ, لأي مصدر إلكتروني أو غير إلكتروني ذا حقوق خاصة.
- يجب الإشارة إلى المراجع والمصادر المستخدمة داخل الأنظمة.

11- التعامل مع الحوادث الأمنية:

- يجب الإبلاغ عن أي نشاط مشبوه فورًا إلى فريق الأمن السيبراني
- يتم التحقيق في الحوادث واتخاذ التدابير التصحيحية المناسبة.
- يتم وضع خطط استجابة للطوارئ لضمان استمرارية الأعمال.

12- التوعية والتدريب:

- يتم تقديم دورات تدريبية دورية لجميع المستخدمين حول أفضل ممارسات الأمن السيبراني.
- يجب على كل مستخدم الالتزام بالإجراءات الأمنية المعتمدة.
- يتم إرسال نشرات توعوية على قنوات التواصل المتاحة.

13- الامتثال والمراقبة والتحديثات والمراجعة:

- يتم إجراء مراجعات دورية لضمان الامتثال لهذه السياسة.
- يخضع أي انتهاك لهذه السياسة لإجراءات تأديبية وفقًا للوائح مدارس دلتا.
- تتم مراجعة سياسة الأمن المعلوماتي بشكل دوري لضمان مواكبتها لأحدث التطورات في مجال الأمن السيبراني.
- سيتم عمل التعديلات عند الحاجة لضمان بيئة آمنة لجميع المستخدمين, وبعدها يتم أخذ الموافقة اللازمة ونشر لتلك التعديلات.

الإطار التنظيمي:

الدور	المسؤولية
الإدارة العليا	• الاعتماد • الإشراف على تنفيذ السياسة • تعميم السياسة على المجتمع المدرسي
قسم تقنية المعلومات	• نشر الثقافة و المعالجة • المسؤول عن التنفيذ،التحديث التطوير • مراقبة الحوادث الأمنية والاستجابة لها
الموظفون والمعلمون والطلاب	• الالتزام بتطبيق السياسة

جدول التعريفات:

المصطلح	التعريف
الأمن السيبراني	حماية الأنظمة والشبكات من الهجمات الرقمية

البيانات الحساسة	المعلومات التي يجب حمايتها من الوصول غير المصرح بمراقبة الحوادث الأمنية والاستجابة لها
التشفير	تقنية لحماية البيانات بجعلها غير قابلة للقراءة بدون مفتاح خاص

جدول الاختصارات:

الاختصار	المعنى
ISO	المنظمة الدولية للتوحيد القياسي
ITIL	مكتبة البنية التحتية لتكنلوجيا المعلومات
COBIT	إطار حوكمة تكنلوجيا المعلومات
CIS	مكز أمان الإنترنت