سياسة أمن المعلومات الإلكترونية

تفاصيل السياسة	
عنوان السياسة	سياسة أمن المعلومات الإلكترونية
رقم السياسة	GP-26-10
مجال السياسة (اختر مجالاً واحدًا)	■ حوكمة ☐ أكاديمي ☐ إداري
	☐ بحثي ☐ شؤون الطلبة
مالك السياسة	سعادة رئيس الجامعة
حالة السياسة	■ سياسة جديدة ☐ تعديل رئيسي ☐ تعديل ثانوي
سلطة الاعتماد	مجلس الجامعة
حالة الاعتماد	■ معتمدة ☐ قيد المراجعة
تاريخ الاعتماد	10 May2026
جهة الاتصال الرئيسية	نور بنت سليمان السيفية -رئيسة قسم أمن المعلومات الإلكترونية
عنوان البريد الإلكتروني	Noor.alsaifi@utas.edu.om
رقم جهة الاتصال	+96824114202

التحكم في الإصدار

رقم الإصدار	معتمدة V1
تاريخ المراجعة القادم	10May 2029
جهة المنشأ/ الإصدار	قسم أمن المعلومات الإلكترونية
المراجعون	Academic Council

التغذية الراجعة والتقييم

رقم الإصدار	تاريخ المراجعة	ملخص المراجعة والتغذية الراجعة
v0.1 (Draft)	٢٠٢٤/٠٢/١٨	فرع الجامعة بصلالة: بعض المقترحات وتم اضافتها في السياسة.
v0.1 (Draft)	٢٠٢٤/٠٥/١٦	مركز الدفاع الإلكتروني: اقتراح تعديلات لغوية في صياغة السياسة -تم تعديلها اضافة بعض التعريفات -تمت الاضافة
v0.1 (Draft)	07/10/2024	فرع الجامعة بالمصنعة: • تم توضيح بعض المقترحات في السياسة - تم الأخذ بالمقترحات • تم إعادة صياغة بعض الجمل.
V01 (Draft)	19/08/2024	دائرة الجودة: تعديل تنسيق محتوى السياسة – تم التعديل اقتراح بعض التعديلات اللغوية – تم التعديل

التحقق من الانتحال

رقم الإصدار	التاريخ	نسبة التشابه	ملاحظات
v0.1 (Draft)	19/08/2024	%3	-

التدقيق اللغوي

رقم الإصدار	التاريخ	مراجعة وتدقيق لغوي:	ملاحظات
v0.1 (Draft)	8 نوفمبر 2025	د. ابراهيم بن محمد الحارثي	-
V0.1(Draft)	9 نوفمبر 2025	نور بنت سليمان السيفية	-
V0.1(Draft)	مارس ٢٠٢٦	فريق هيكلة السياسات	دمج عدد من السياسات

التوقيع والختم

جامعة التقنية والعلوم التطبيقية
University of Technology and Applied Sciences
مكتب الرئيس

جامعة التقنية والعلوم التطبيقية
University of Technology and Applied Sciences

الفهرس

سياسة أمن المعلومات الإلكترونية

١- الغرض

تهدف سياسة أمن المعلومات الإلكترونية إلى حماية البيانات والمعلومات الرقمية الخاصة بالجامعة من الوصول غير المصرح به، أو التعديل، أو الإتلاف، أو الإفشاء، بما يضمن سرية المعلومات وسلامتها وتوافرها. تسعى هذه السياسة إلى وضع إطار واضح لإدارة المخاطر المرتبطة بالأمن السيبراني، وتعزيز ثقافة الوعي الأمني لدى جميع منسوبي الجامعة. كما تحدد هذه السياسة المسؤوليات والالتزامات لضمان الامتثال للمعايير الوطنية والدولية، بما يحقق حماية البنية التحتية التقنية ودعم استمرارية الأعمال الأكاديمية والإدارية.

٢- نطاق السياسة

تنطبق هذه السياسة على جميع الأنظمة الإلكترونية، الشبكات، الأجهزة، التطبيقات، وقواعد البيانات التي تمتلكها أو تديرها الجامعة، وكذلك على جميع المستخدمين الذين لديهم حق الوصول إلى موارد المعلومات الإلكترونية، بما في ذلك أعضاء هيئة التدريس، الموظفين، الطلاب، والمتعاقدين الخارجيين. تشمل السياسة جميع الأنشطة المتعلقة بجمع، تخزين، معالجة، نقل، أو مشاركة المعلومات الإلكترونية داخل الجامعة أو عبر شبكاتها. لا تغطي هذه السياسة الأنظمة أو الأجهزة الشخصية التي لا ترتبط بشبكة الجامعة أو لا تستخدم في الوصول إلى مواردها، إلا إذا تم استخدامها لمعالجة بيانات الجامعة أو الوصول إلى خدماتها.

٣- بيان السياسة

تلتزم الجامعة بتطبيق أعلى معايير أمن المعلومات لحماية بياناتها وأنظمتها الإلكترونية من أي تهديدات أو استخدام غير مصرح به، بما يضمن سرية المعلومات وسلامتها وتوافرها. تعتمد

هذه السياسة على مبادئ الحوكمة الأمنية، وإدارة المخاطر، والامتثال للأنظمة الوطنية والمعايير الدولية ذات الصلة.

على جميع المستخدمين بالجامعة، بما في ذلك أعضاء هيئة التدريس، الموظفين، الطلاب، والمتعاقدين، الالتزام التام بهذه السياسة عند استخدام موارد المعلومات الإلكترونية الخاصة بالجامعة. وتشمل الأنشطة التي تغطيها السياسة:

- الوصول إلى الأنظمة والشبكات والتطبيقات التابعة للجامعة.
- تخزين ومعالجة ونقل المعلومات الإلكترونية.
- استخدام الأجهزة والبرمجيات المرتبطة بالبنية التحتية التقنية للجامعة.

تفرض هذه السياسة قيودًا واضحة على أي سلوكيات قد تعرض أمن المعلومات للخطر، مثل مشاركة كلمات المرور، تثبيت برامج غير مصرح بها، أو محاولة الوصول إلى بيانات أو أنظمة دون إذن. ويجب على جميع الأطراف المعنية الامتثال للإجراءات الأمنية المعتمدة لضمان حماية المعلومات واستمرارية الخدمات.

٤- الجهات والمسؤوليات والتفويض

الجدول الآتي يوضح الأدوار والمسؤوليات للامتثال لسياسة أمن المعلومات الإلكترونية بالجامعة:

المهام	المسؤوليات
قسم أمن المعلومات الإلكترونية	• إعداد السياسة • الإشراف على تنفيذ السياسة ومتابعة الامتثال . • إجراء تقييمات دورية للمخاطر وتقديم تقارير للإدارة العليا . • تنظيم برامج تدريبية وتوعوية لجميع المستخدمين.
الادارة العليا	• اعتماد سياسة أمن المعلومات الإلكترونية وتوفير الموارد اللازمة لتطبيقها. • دعم تنفيذ الإجراءات الأمنية وضمان الامتثال للأنظمة واللوائح ذات الصلة.

التقسيمات الإدارية والأكاديمية بالجامعة ذات العلاقة بتطبيق السياسة	• تطبيق وتنفيذ والامتثال للضوابط المحددة بالسياسة. • الإفصاح عن أي حوادث أمنية أو خروقات أمنية إلى قسم أمن المعلومات الإلكترونية.
الأكاديميون والموظفون	• الالتزام بالسياسة عند استخدام الأنظمة الإلكترونية والبيانات الخاصة بالجامعة. • الامتثال لهذه السياسة وضوابطها وإجراءاتها. • الإبلاغ الفوري عن أي حادث أمني أو نشاط مشبوه لإدارة قسم أمن المعلومات الإلكترونية.
الطلاب	• استخدام موارد الجامعة الإلكترونية وفق الضوابط المحددة في السياسة. • الحفاظ على سرية بيانات الجامعة وعدم إساءة استخدام الأنظمة. • الامتثال لهذه السياسة وضوابطها وإجراءاتها. • الإبلاغ الفوري عن أي حادث أمني أو نشاط مشبوه لإدارة قسم أمن المعلومات الإلكترونية.
المتعاقدون ومقدمو الخدمات الخارجية	• الالتزام والامتثال لهذه السياسة عند التعامل مع أنظمة أو بيانات الجامعة. • توقيع اتفاقيات سرية وضمان الامتثال للمعايير الأمنية المعتمدة بالجامعة.

٥- السياسة

سياسة أمن المعلومات الإلكترونية هي مجموعة من المبادئ والضوابط التي تضعها الجامعة بهدف حماية بياناتها وأنظمتها الإلكترونية من التهديدات والمخاطر، سواء كانت داخلية أو خارجية. تحدد هذه السياسة الإطار العام لإدارة أمن المعلومات، وتشمل حماية سرية وسلامة وتوافر المعلومات، والالتزام بالأنظمة الوطنية والمعايير الدولية الخاصة بأمن المعلومات، وتطبيق ضوابط الوصول الآمن إلى الأنظمة والبيانات وإدارة المخاطر والاستجابة للحوادث الأمنية بشكل فعال.

هذه السياسة هي المرجع الأساسي الذي يوضح موقف الجامعة وتوقعاتها فيما يتعلق باستخدام وحماية المعلومات الإلكترونية، لضمان استمرارية الأعمال الأكاديمية والإدارية بأمان.

٥-١ التعريفات

٥-١-١ **أمن المعلومات:** حماية المعلومات من الوصول غير المصرح به، أو التعديل، أو الإتلاف، أو الإفشاء، بما يضمن سرية المعلومات وسلامتها وتوافرها.

٥-١-٢ **المعلومات الإلكترونية:** جميع البيانات والمحتويات المخزنة أو المعالجة أو المنقولة عبر الأنظمة الإلكترونية التابعة للجامعة.

٥-١-٣ **المستخدمون:** جميع الأشخاص الذين لديهم حق الوصول إلى موارد المعلومات الإلكترونية الخاصة بالجامعة، بما في ذلك أعضاء هيئة التدريس، الموظفين، الطلاب، والمتعاقدين.

٥-١-٤ **البيانات الحساسة:** أي معلومات تتعلق بالطلاب، الموظفين، الأبحاث، أو الشؤون المالية التي قد يؤدي كشفها أو تعديلها إلى ضرر للجامعة أو الأفراد.

٥-١-٥ **التهديدات الأمنية:** أي حدث أو نشاط يمكن أن يؤدي إلى اختراق، أو فقدان أو تلف المعلومات أو الأنظمة الإلكترونية.

٥-١-٦ **الحوادث الأمنية:** أي خرق أو محاولة خرق للسياسات الأمنية، مثل الوصول غير المصرح به أو تسريب البيانات.

٥-١-٧ **ضوابط الوصول:** الإجراءات والتقنيات المستخدمة لتقييد الوصول إلى المعلومات والأنظمة بناءً على الصلاحيات الممنوحة.

٥-٢ الاجراءات :

تشمل هذه السياسة تنفيذ وتطبيق مجموعة من الإجراءات والضوابط الأمنية التي تهدف إلى حماية المعلومات وأصول التقنية لدى الجهة، وتشمل – على سبيل المثال لا الحصر – ما يلي:

- إجراءات أمن الشبكات وأمن الأنظمة والتطبيقات.
- إجراءات الأمن المادي والبيئي.
- إجراءات الاستجابة للحوادث الأمنية وإدارتها.

- إجراءات التوعية والتثقيف الأمني للمستخدمين.
- إجراءات الاستخدام الآمن والأخلاقي لتقنيات الذكاء الاصطناعي.

كما تلتزم الجامعة بالامتثال التام لكافة الضوابط والمعايير والتعليمات والتعاميم الصادرة عن الجهات المنظمة للأمن السيبراني في سلطنة عُمان، مع الالتزام بتطبيق القوانين والتشريعات المعمول بها في سلطنة عُمان عند التعامل مع أي تجاوزات أو مخالفات أمنية.

٥-٣العناصر الأخرى ذات الصلة

- **الامتثال والإنفاذ:** في حال عدم الامتثال للسياسة ستطبق القوانين والعقوبات حسب الانظمة والقوانين المعمول بها في سلطنة عمان.

٦- المراجع

1. Cyber Defence Centre. (2022). National Strategy for Cyber Defence (2022-2025). https://cdc.gov.om/files/strategy.pdf
2. Royal Decree No. 12/2011 (2011). The Law on Combating Cybercrime. 929, 2–15. https://cdc.gov.om/files/The Cyber Crime Law_Ar.pdf
3. Cyber Defence Centre. (2023). Mandates and Authorities of the Units Responsible for Information Security. https://cdc.gov.om/files/rolesandpermissions.pdf
4. ITA. (2018). IT Risk Management Framework. 1–8. https://oman.om/wps/wcm/connect/18655e32-ea30-4dd9-8b51-4023051aa223/Information+Security+Management+Framework Final+draft.pdf?MOD=AJPERES&CACHEID=18655e32-ea30-4dd9-8b51-4023051aa223
5. ITA Oman. (2016). General Information Security Policy. 0–38.
6. MoE. (2013). Information Security Guidelines. https://home.moe.gov.om/file/main-tab/secrity policy.docx
7. MTICT. (2014). General Policy of Information Security. https://www.mtcit.gov.om/ITAPortal_AR/Pages/Page.aspx?NID=2187&PID=389138
8. National Information Security & Safety Authority. (2013). https://nissa.gov.ly/
9. Public Authority of Manpower Register. (2011). https://www.mol.gov.om/
10. https://www.ita.gov.om/ITAPortal/MediaCenter/Document_detail.aspx?NID=115

٧- الملاحق

ستكون الملاحق مرفقة مع ملفات الإجراءات المنفصلة.