جامعة التقنية
والعلوم التطبيقية
University of Technology
and Applied Sciences

E-INFORMATION SECURITY POLICY

POLICY DETAILS			
Policy Title	E-INFORMATION SECURITY POLICY		
Policy Number	GP-26-10		
Policy Area (Choose one)	■ Governance	☐ Academic	☐ Administrative
	☐ Research	☐ Student Affairs	
Policy Owner(s)	H. E. Vice Chancellor		
Policy Status	■ New Policy	☐ Major Amendment	☐ Minor Amendment
Approval Authority	University Council		
Approval Status	■ Approved	☐ Under Review	
Approval Date	10th May 2026		
Lead Contact	Noor Sulieman Al-Saifi, Head of Information Security Office		
E-mail Address	Noor.alsaifi@utas.edu.om		
Contact Number	24114202		

VERSION CONTROL

Version No.	v1.0 (Final)
Date of Next Review	10th May 2029
Unit of Origin	E-Information Security
Reviewers	Noor Sulieman Al-Saif- HO

Feedback And Amendments

Version No.	Date	Summary of Revisions or Feedback
v0.1 (Draft)	18/02/2024	The university branch in Salalah: Some suggestions were made and added to the policy
	16/05/2024	Cyber Defense Center: Proposed linguistic edits to the policy wording — completed. Addition of several definitions — completed.
v0.2 (Draft)	07/10/2024	University Branch in Al-Musannah: • Some suggestions were clarified in the policy — the suggestions were adopted. • Some sentences were rephrased.
	19/08/2024	Quality Department: • Adjustment of the policy content formatting — completed. • Proposed some linguistic modifications — completed.
v0.3 (Draft)	25/05/2025	Academic Council decision to develop one policy and append all the other policies to this policy.

Plagiarism Verification

Version No.	Date	% Of Similarity	Remarks
v1.0 (Final)	25-06-2026	18%	

Proofreading

Version No.	Date	Proofread By:	Remarks
v1.0 (Final)	25/03/2026	Noor Sulieman Al-Saif	Policy team member
v1.0 (Final)	26/03/2026	Dr. Ibrahim Alharthy	Policy development team member

SIGNATURE AND STAMP

TABLE OF CONTENTS

E-INFORMATION SECURITY POLICY

1. PURPOSE

The E-Information Security policy aims to protect digital data and information from unauthorized access, modification, damage, or disclosure, ensuring its confidentiality, integrity, and availability. This policy establishes a clear principle for managing cybersecurity risks and fostering a culture of security awareness among all university members. It also defines responsibilities and obligations to ensure compliance with Omani national and international standards, thereby protecting the university technological infrastructure and supporting the continuity of its academic and administrative operations.

2. SCOPE

This policy applies to all electronic systems, networks, devices, applications, and databases owned or operated by UTAS, as well as to all users with access to electronic information resources, including faculty, staff, students, and external contractors. The policy covers all activities related to the collection, storage, processing, transmission, or sharing of electronic data or information within the university or across its networks. This policy does not cover personal systems or devices that are not connected to the university network or used to access its resources, unless they are used to process university data or access its services.

3. POLICY STATEMENT

UTAS is committed to implementing the highest information security standards to protect its data and electronic systems from threats and unauthorized use, ensuring the confidentiality, integrity, and availability of its information. This policy is based on the principles of security governance, risk management, and compliance with relevant Omani national regulations and international standards.

All university users, including faculty, staff, students, and contractors, must fully comply with this policy when using UTAS electronic information resources. Activities covered by the policy include:

- Accessing UTAS systems, networks, and applications.
- Storing, processing, and transmitting electronic information.
- Using hardware and software related to the university's technological infrastructure.

E-Information Security policy imposes clear restrictions on any behaviors that could compromise information security, such as sharing passwords, installing unauthorized software, or attempting to access data or systems without authorization. All parties involved must comply with the approved security procedures to ensure information protection and service continuity.

4. AUDIENCE, RESPONSIBILITIES AND DELEGATION

The following table outlines the roles and responsibilities for complying with UTAS E-Information Security policy:

ROLES	RESPONSIBILITIES
E-Information Security Department	• Policy development. • Policy implementation and monitoring compliance. • Conducting periodic risk assessments and reporting to senior management. • Organizing training and awareness programs for all users.
Deputies/Assistants of the Vice-Chancelor	• Adopting E-Information Security policy and providing the necessary resources for its implementation. • Supporting the implementation of security measures and ensuring compliance with relevant regulations and laws.
Administration and Academic Departments	• Implement, enforce, and comply with the controls outlined in the policy. • Report any security incidents or breaches to the Cybersecurity Department.

University Staff	• Adhere to the policy when using university electronic systems and data. • Comply with this policy, its controls, and procedures. • Immediately report any security incident or suspicious activity to the Electronic Information Security Department.
Students	• Use the university's electronic resources in accordance with the guidelines outlined in this policy. • Maintain the confidentiality of university data and refrain from misusing the systems. • Comply with this policy, its controls, and procedures. • Report any security incident or suspicious activity to the Information Security Department immediately.
Contractors and External Service Providers	• Adherence to and compliance with this policy when handling university systems or data. • Signing confidentiality agreements and ensuring compliance with UTAS-approved security standards.

5. POLICY

The following key principles outline the university's approach to safeguarding electronic information and systems, ensuring compliance, and maintaining secure operations:

- Protect university data and electronic systems from internal and external threats through the application of comprehensive guidelines and controls.
- Ensure confidentiality, integrity, and availability of information by adhering to Omani national laws and international information security standards.
- Implement secure access controls for systems and data to manage risks and respond effectively to security incidents.

- Establish this policy as the foundational reference for the university's stance and expectations on the use and safeguarding of electronic information, assuring the secure continuity of academic and administrative functions.

5.1 Definitions:

5.1.1 Information Security: Protecting information from unauthorized access, alteration, destruction, or disclosure, ensuring its confidentiality, integrity, and availability.

5.1.2 Electronic Information: All data and content stored, processed, or transmitted through the university's electronic systems.

5.1.3 Users: All people with access to the university's electronic information resources, including faculty, staff, students, and contractors.

5.1.4 Sensitive Data: Any information relating to students, staff, research, or financial matters, the disclosure or alteration of which could cause harm to the university or individuals.

5.1.5 Security Threats: Any event or activity that could lead to breach, loss, or damage to information or electronic systems.

5.1.6 Security Incidents: Any breach or attempted breach of security policies, such as unauthorized access or data leaks.

5.1.7 Access Controls: The procedures and techniques used to restrict access to information and systems based on granted permissions.

5.2 Procedures

Compliance and Enforcement:

This policy includes the implementation and enforcement of a set of security procedures and controls aimed at protecting the organization's information and technological assets. These include, but are not limited to, the following:

- Network security and Systems, applications security procedures.
- Physical and environmental security procedures.
- Security incident response and management procedures.
- Security awareness and training procedures for users.
- Procedures for the safe and ethical use of artificial intelligence technologies.

6. REFERENCES

SN	Institution Name	Referenced Points
1	Cyber Defense Centre	Cyber Defense Centre. (2022). National Strategy for Cyber Defense (2022-2025). https://cdc.gov.om/files/strategy.pdf
2	https://cdc.gov.om	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 Defense Centre	Cyber Defense Centre. (2023). Mandates and Authorities of the Units Responsible for Information Security. https://cdc.gov.om/files/rolesandpermissions.pdf
4	ITA Oman	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	ITA Oman. (2016). General Information Security Policy. 0–38.
6	MoE Oman	MoE. (2013). Information Security Guidelines.

		https://home.moe.gov.om/file/main-tab/secrity policy.docx
7	MTICT Oman	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.	National Information Security & Safety Authority. (2013). https://nissa.gov.ly/
9	Public Authority of Manpower Register	Public Authority of Manpower Register. (2011). https://www.mol.gov.om/ 10.https://www.ita.gov.om/ITAPortal/MediaCenter/Document_detail.aspx?NID=115

7. APPENDICES

- The appendices will be attached to the separate procedural files.