DAU 7-1 Cyber Security Policy

Policy Code	Policy Name		
DAU 7-1	Cyber Security Policy		
Responsible Executive		**Current Revision Date**	**Next Revision Date**
Information Technology (IT) Department		10/2023	10/2027

1. Policy Purpose

This policy informs all DAU members, students and visitors of their responsibilities related to maintain the privacy and security of institutional information and the information technology resources. Protection of information and information technology resources is critical to ensure the confidentiality, integrity, and availability of the information.

2. Policy Scope

This policy applies to all faculty staff, students, employees, and any other individuals who have access to university-owned technology resources and devices. This policy is applied as well on the IT Facilities and Services such as: (telecommunication and network equipment, desktop/laptop computers, mobile devices, servers, storage solutions, software packages, and applications which are owned by or operated on behalf of DAU, its component institutions, or any of its administrative, academic) at the university.

3. Policy Statement

The University aims to maintain an appropriate level of Cyber Security to ensure the confidentiality, integrity, and availability of all electronic Services.

4.Policy Procedure

The following section shows some of the information technology risks related to Cyber- Security:

- Hacking:

DAU uses effective and strong anti-hacking systems with professional IT employees to avoid such risk and to ensure safety of students' and employee's data and records.

- Virus attacks:

DAU's employees use certified, original, and effective Anti-Virus programs to prevent such risks, this software is downloaded on all DAU's computers in laboratories and for employees.

- Access of Unauthorized Users:

All Unauthorized Users are banned from utilizing DAU Information Technology services for any purpose. Unauthorized PSU users can receive disciplinary actions which may lead to employment termination.

- Using Non-Genuine Software:

Un-genuine downloaded programs and software will cause the easy malware infection of computers and laptops and for the stored data on these devices. So that, DAU always buys and uses the original programs and software within the university in addition to purchasing PCs and laptops from trusted vendors. Also, DAU always renews, and rebuys expired programs and software. DAU doesn't permit any purchasing or downloading any non-genuine software and programs.

- Data Theft and stolen:

Data theft is the act of stealing digital information stored on computers, servers, or electronic devices to obtain confidential information or compromise privacy. The data stolen can be anything from bank account information, online passwords, passport numbers, social security numbers, medical records, online subscriptions, and so on. Data that may be stollen at DAU may be one of the following:

- DAU Students records and information.
- Financial Data such as credit card or debit card information.
- Proprietary process descriptions and operating methodologies.
- Network credentials such as usernames and passwords.
- DAU employees' records, data, and information.

- Human Errors:

Some human errors may occur such as setting wrong exam grade on the system, or any other human errors related to personal data for employees and students. IT responsible in DAU has the access to change and modify the data with mistake after formal request and approval from the authorized personnel in DAU, and the record of the data changed or modified shall be kept in IT.

DAU ensures its Cyber Security system by the conducting the following procedure:

- DAU IT security team will conduct regular risk assessments to identify and prioritize cybersecurity risks. The IT security team will develop measures to reduce identified risks and will report to the IT Director on the risk assessment results and proposed remediation actions. Cyber security controls seek to reduce cyber security risk by either reducing the likelihood or impact of an incident, or both. DAU IT team on a regular basis conducts Cyber Security Risk Management controls and measuring its effectiveness.
- Access to university IT assets, including user accounts, systems, and data, will be granted in accordance with established procedures. The IT security team will manage user access controls and monitor user activity for suspicious behavior. Access to sensitive data will be restricted to authorized personnel only.
- DAU's network infrastructure will be secured through the implementation of firewalls, intrusion detection and prevention systems, and network segmentation. The IT security team will monitor network activity for security threats and vulnerabilities and will implement controls to protect against unauthorized access and data exfiltration.
- The university will establish procedures for responding and solving cybersecurity incidents, including reporting and escalation procedures, incident investigation and analysis, as well as communication with stakeholders if needed.
- The university's cybersecurity program will comply with relevant laws and regulations, such as data privacy regulations and industry-specific compliance requirements.
- The IT security team will monitor compliance and implement necessary controls and procedures to ensure compliance with all applicable regulations.

Cybersecurity Preventative Procedure within DAU

Cyber Security Preventative Procedures are crucial in DAU as it ensures minimizing the Cyber Security risks within DAU. These preventive actions conducted through:

- Next-Generation Firewall: The University uses NGFW firewall appliance to log and protect internet and network usage, including connectivity of all Authorized Users and Digital Services, to prevent known threats and vulnerabilities from being exploited.
- Blocking of websites: The University blocks certain website URLs, as their content is considered unsafe, unacceptable, or would put people, Digital Services, or the University at risk. This includes, but is not limited to, malicious, gambling, pornographic, or terrorist content.

- Blocking of applications: The University occasionally places a throttle or limit on the internet traffic to certain high bandwidth streaming applications to prevent an unnecessary drain on University Digital Services.
- Antivirus software's: The University uses antivirus software to ensure the confidentiality, integrity, and availability of its Digital Services and detect any malware or similar malicious code.
- Automated Spam and Phishing detection: The University uses systems that detect spam, phishing messages, and other malicious email entering and leaving its email servers, to protect against Spam, Phishing attempts and viral outbreaks.
- Password strength: The University requires a certain level of complexity in all Authorized Users' passwords. DAU insists on using strong passwords to avoid any data theft and it doesn't permit using the same passwords for different users or programs.
- Secure Sockets Layer (SSL): which is a security protocol that provides privacy, authentication, and integrity to Internet communications which DAU uses to issue cryptographic certificates.
- Monitoring of logs: IT conducts routine monitoring of Digital Services and logs related to those services. This monitoring may reveal signs of external interference, including foreign interference, which is handled in accordance with the Cyber Security Incident Management Process.
- Data Accuracy: All students' and employees' data shall be confidential and accurate. IT on a regular basis review this data to ensure its consistency. Only authorized personnel in DAU can have access to these data.

5. Related Policies/ Documents/ Forms

DAU 7-5 IT Technical Support Policy
DAU 7-7 Use of Technology Resources

6. Document History

Version	Issue/ Rev. Date	Updated Information/ Summary of Changes
1	10/2023	1st issue of the policy