STARDOM UNIVERSITY

Policies, Systems, and Regulations Guide

Information Security Policy

Issued pursuant to Article (16) of the Academic Policies, Regulations, and Bylaws of 2024

Approval of the University Board of Directors No. (65)

2024/07

Politics

Information security

Stardom University Private

Executive Summary

Information is an important and vital component of any organization, especially in academic institutions like Stardom University, where knowledge is its most important driver. Information is linked to learning, teaching, research, studies, management, and organization. Therefore, it is essential that computer data, hardware, networks, and software are adequately protected against alteration, damage, theft, or unauthorized access.

Stardom University is committed to protecting information assets and resources that are essential to academic and research activities. These information assets (including its networks) will be protected by controlling authorized access, establishing logical and physical barriers to unauthorized access, and developing an integrated security system to protect hardware, software, networks, and applications.

An effective information security policy provides a sound basis for defining, regulating, and adequately protecting the management of corporate information assets and information systems that transmit, process, and store corporate data from negative impacts that compromise confidentiality, integrity, and availability.

This policy requires that information security practices be integrated into the daily use of university systems.

Information Security Policy Objectives

The University is committed to protecting the security of its information systems and information and ensuring that users have access to the information they need to do their work. Information underpins all of the University's activities and is essential to its research, educational, and administrative functions. The following are the objectives of the Information Security Policy:

1. Maintain the confidentiality, integrity and availability of Stardom University's information assets.
2. Protecting the academic, administrative and personal information of employees and students from hacking and threats.
3. Preventing data loss, modification, and dissemination, including research and teaching.
4. Protecting information security from incidents that may harm the university's business, reputation, and professional standing.
5. Knowing and defining responsibilities and accountability for information security.

Information Security Principles

It includes knowledge of university information resources, allowing access to all authorized users, and ensuring the proper and appropriate handling of information. The university has adopted the following principles upon which this policy is based:

• AInformation that constitutes an important asset to the university system and a valuable asset that must be protected.

- The systems used to transmit, process and store this information must be protected.
- Information should be available to all authorized users and protected against unauthorized access.
- Information must be classified according to its sensitivity and value as stated in the Data Classification Policy.
- The integrity of information must be maintained so that information is accurate, complete, timely, and consistent with other information.
- All university system users who have access to information have a responsibility to handle it appropriately, according to its classification.

• ACompliance with this policy is mandatory for the Stardom University community.

Policy outcomes

By enforcing the data classification policy, we seek to achieve the following results:

1. Managing potential risks that threaten the university's information security and reducing the possibility of their occurrence and misuse of information.
2. Achieving credibility and transparency with community organizations and Stardom University partners.
3. Protecting information and data from loss, manipulation, and misuse at all stages of use and during circulation.

Rationale Policy

Stardom University possesses information that is considered sensitive and valuable, ranging from personal information, research, and other information considered sensitive to financial data. This information needs to be protected from unauthorized use, modification, disclosure, or destruction.

The transfer of sensitive information between unauthorized individuals could harm the university community or the university. Additionally, if university information is tampered with or made unavailable, it could damage the university's reputation and call into question its transparency and integrity.

Therefore, all employees of the university system are required to protect information in a manner commensurate with its level of sensitivity. The information security policy has been developed in accordance with the principles and guidelines in a document entitled "Data Classification Policy."

General Policy Statement

Information is essential to the effective functioning of the University and is a critical business asset. The purpose of this Information Security Policy is to ensure that the information managed by the University is appropriately secured to protect against the potential consequences of breaches of confidentiality, failures of integrity, or interruptions in the availability of that information. Any reduction in the confidentiality, integrity, or availability of information could prevent the University from operating effectively and efficiently.

Application

This policy applies to all individuals, whether employees, students, consultants, or other groups who are granted access to information and information and communication technology systems at the university.

Security roles and responsibilities

All members of the University who have direct or joint responsibility for processing information or using the University's information resources and systems are bound by this policy and other relevant policies. In order to fulfill these responsibilities, members of the University must:

- Be aware of and comply with this policy.
- Understanding and knowing the nature of the information to which they have the right to access.

• ATo learn about the information systems and computers for which they are responsible.