STARDOM UNIVERSITY

Policies, Systems, and Regulations Guide
Access Control 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

policy

Entry control

Stardom University

the introduction

Stardom University is a leading online university that relies on e-learning and blended learning for its educational process. This system contains a wealth of information and data related to staff, students, and academic research, which could be vulnerable to hacking and misuse, posing a serious threat to student privacy and data. Hence, the need to develop an access control policy to ensure adequate protection of personal information and provide an easy and quick way to log in to the student system.

This guide aims to provide cybersecurity requirements to mitigate risks associated with the use of Stardom University's systems and assets and protect them from internal and external threats. The guide focuses on maintaining the confidentiality, integrity, and availability of information, as well as compliance with cybersecurity requirements and relevant legislative and regulatory requirements, as part of the basic cybersecurity controls.

This policy covers all information and technology assets and services provided via the Internet, including websites, web applications, smartphone and tablet applications, email, and remote access. This policy applies to all university employees, both direct and indirect, as well as to third-party employees permitted to use university-owned information and systems.

Policy objectives

- Reducing cyber risks and resulting privacy violations.
- Establish controls over account access based on business and security requirements.
- Documenting formal procedures for controlling user access.
- Maintaining information and protecting its confidentiality, integrity, and availability on the university's network and systems.

Access Control Policy Terms

Create and modify accounts

- Define, document, and approve cybersecurity requirements for login management, identifying and authorizing username and password-based access.
- Create unique, non-duplicate accounts to ensure users' identities are identified while using university systems.
- Systems administration uniquely identifies and authenticates all users before granting them access to the system.
- Conduct periodic reviews of user accounts and attach a unique reference number to each user account creation request to ensure traceability.
- Document procedures for handling service accounts and ensure they are managed securely between applications and systems.
- Allow the creation of shared email accounts and mailboxes, provided that one owner is designated for each account to ensure traceability and accountability.
- Suspend the accounts of old or resigned students and withdraw all their privileges.
- Modify employee permissions based on the job changes assigned to them.

User password management

- Prevent sharing your password via any means, including email and voice calls.
- Choose passwords that are different from those used for personal accounts.
- Account disabled after three failed login attempts.
- Use multi-factor authentication or two-factor authentication systems for sensitive data.
- Follow standard criteria for choosing a username and password in terms of length and complexity.
- Allow users to change their passwords.
- Do not store passwords as clear text, but encrypt them.
- Save the password age and history and prevent using the same password before.
- Force users to change temporary passwords upon their first login.

Privileges Management

- Restrict access to operating systems and applications to responsible system administrators and support staff.
- Grant privileges to users based on their supervisor's authorization and in accordance with their job duties.
- Periodically evaluate user privileges and take necessary actions based on the evaluation results.
- Use elevated privileged accounts only when necessary, and avoid using them for routine procedures.
- Train users of privileged accounts and make them aware of the sensitivity of their accounts and the responsibilities that arise from misuse.
- Protect and change passwords for privileged accounts periodically.
- Create and activate university or contract user accounts for specific periods of time, and delete them when no longer needed.
- Suspending employee accounts in the event of a disciplinary penalty being issued against them before notifying them.
- Prevent the use of shared accounts to access information and technical assets and restrict them to specific permissions.

Review login permissions

- Review user access rights and privileges at least once a year.
- Restrict privileges if any misuse is detected.
- Record all failed and successful access attempts and review them periodically.

Exceptions

- All university employees must adhere to these policies. Any exceptions must be authorized by the IT Department.
- Refer to the IT Department and request prior authorization before introducing any third party and granting them access to the university system.

Penalties

- In the event of any intentional or negligent violation, appropriate disciplinary action will be taken in accordance with the university's rules and regulations.