Guidelines and Procedures for End User Access Management in University's Administrative Systems

1. Purpose

The purpose of this document is to establish guidelines on procedures for managing end user access to the University's administrative systems. This is to ensure that access is granted appropriately, maintained securely, and revoked when necessary.

2. Scope

This policy applies to all administrative units and departments that utilize the university's administrative systems, including but not limited to academic staff, administrative staff, IT personnel, and management.

3. Access Control Policy

3.1 Access Levels

- **Full Access**: Granted to users who require full access to all features of the system for management and oversight.
- **Limited Access**: Granted to users who need specific functionalities to perform their job duties but not requiring administrative controls.
- **Read-Only Access**: Granted to users who need to view data without the ability to modify it.

3.2 Department-Specific Access

Users will have access only to the systems and data relevant to their specific department. This ensures that sensitive information is only available to those who need it for their work.

4. User Access Request Process

4.1 Request Submission

- Access requests must be submitted via the Access Request Form available on respective administrative system website.
- Requests must include the user's name, department, role, and specific access level needed.

4.2 Approval Process

- Access requests must be approved by the user's direct supervisor and the department head.
- The concerned system owner will review and process the request within five business days.

5. Access Review

5.1 Regular Audits

- Access permissions will be reviewed annually by the system owner to ensure compliance with this policy.

- Any necessary adjustments will be communicated to the relevant supervisors.

5.2 Termination of Access

- User access must be revoked immediately upon termination of employment or transfer to another department.
- Supervisors must notify system owner within 24 hours of a user's departure or role change.

6. Data Security and Confidentiality

6.1 Data Handling

- Users must handle all data in line with the university's data protection policies.
- Sharing of login credentials is strictly prohibited.

6.2 Incident Reporting

- Any security incidents or breaches must be reported immediately to the IT department for investigation and resolution.

This document serves as a guideline to ensure a secure and efficient access management process for the University's Administrative Systems.