Policy Title	Access Control Policy
Responsible AIU Office **(Higher Management/Directorate)**	Campus Access Control Office (CACO)
Policy Owner **(Executive Department/Office)**	Department Access Controllers (DAC) Campus Access Control Leaders (CACLs)
Pertinent Dates	Created 12-03-2022

I. SCOPE OF POLICY

A comprehensive access control policy will aid in providing a safe and secure learning environment for the staff and students at Alamein International University. In addition, it will establish the responsibility, eligibility, and approval process for members of the University community to be given access to University property through a variety of means, including access cards. This policy and supporting guidelines set out specific responsibilities, conditions and practices that are designed to address critical access needs in a manner that minimizes risks to personal safety and maximizes physical asset protection.

II. DEFINITIONS

N/A

III. POLICY STATEMENT

The safety and security of the physical space and assets are a shared responsibility of all members of the University community. To meet this obligation, the University has established access control policy provisions to address the hardware, software, operations, integrity and administration of the access control system. Only University authorized access control systems shall be used on University facilities.

IV. RESPONSIBILITIES

This policy applies to all members of Alamein International University main campus community, including staff, students and approved external users, having authorized access to any University owned or leased space on the main campus. It will govern all methods of physical access control including but not limited to mechanical key systems, specialized security access systems, card access control systems, and any system designed to control an area or facility access point.

Responsibilities of All Users
All individuals issued a University access control device are required to:

1. Secure and be responsible for the access control device issued to him/her. Access control devices shall be used ONLY by the individual to whom the access control device was assigned Access control devices MAY NOT be loaned to others.
2. Return excess access control devices to the appropriate Department Access Controllers DAC. Only one access control device per access control system will be assigned to each individual. Individuals who have been assigned more than one device per system may retain a second device if approved by a DAC for their area and following execution of an agreement to pay cost of replacement if not returned prior to end of employment to be deducted from the user's final paycheck or other final payment from the University.
3. Return the access control device to the DAC upon separation from the applicable department. (NOTE: Access control devices are considered University property and individuals may be held responsible for failure to return them at the end of employment).
4. Report the loss or theft of all access control devices to the DAC AND the University Security Department within 24 hours of the discovery of the theft or loss. Individuals with access control devices enabled with other functions will also need to notify each service provider to deactivate the functions.
5. Do NOT prop doors open or leave them unsecured during hours when the facility is normally closed to the public. High risk & security doors should remain locked at all times.
6. Report unusual access control locks or other access activities that appear to be out of the ordinary to the facility DAC or the University Security Department.

V. POLICY STANDARDS AND PROCEDURES

Formatted: List Paragraph, Justified

- Access to Facilities

Access to each building on campus, including access to building perimeters, areas and equipment, will be regulated by the departments that are responsible for the applicable building, in compliance with this policy. The appropriate level of access control is to be determined by the needs, responsibilities and privileges of a given user or group, including the dates and times that the particular user/group requires access.

- Levels of Access and Associated Responsibilities

The user and associated administrative control levels are based on a facility's risk assessment and individual department needs, and each user's level of access is based upon the user's role at the University. Eligibility for access control devices (eg. cards) is determined by the Divisional Access Controller Managers and Department Access Controller for each facility in accordance with a person's access necessity. Some users will require access to a single room (such as a student's access to an assigned room in Housing), while the role of others will necessitate additional levels of access. The level of access allowed for users is at the discretion of the University, and may include the following levels of control and associated responsibility.

- Individual Access. This user is allowed access to a single room.
- Departmental Access. This level of access allows access to all areas within a single department.
- Outside Door Access. This user is allowed access to a specific building from a specific outside door.
- Building/Department Partitioned Operators. This user is allowed access to certain areas within a building or complex, such as a custodial worker assigned to a particular area of campus.
- Divisional/College Access Controller. This user is allowed to provide access to a specific group of individuals within a series of buildings or college. Ex. Housing.

- Coordination Process

1. Departments must obtain written authorization from the applicable dean/director to requisition new access control system components or initiate the modification of an existing access control system

and send the authorization to the University's Maintenance Department with an approved work order. All installation and/or modifications shall be compatible with University access control systems.

2. Departments implement department access control procedures and coordinate associated training with the University's Security Systems Technician.

3. Once the authorization for access control has been issued; Departments must:

a. For electronic access control device:

1) The device holder will bring the device to the authorized partition controller to assign access permission.

2) The controller shall activate access permissions that have been authorized by the department(s) that manages the space, using the campus system software.

3) The controller shall retain a record of the authorization.

b. For every device issued, including keys, etc., the controller shall notify the device holder of his/her responsibilities; and shall retain records that document the device number, name of recipient, date of issue, access permissions given, date of return or loss, and any dates upon which access permissions were suspended or deactivated.

c. Maintain an inventory of and store unassigned department access control devices in a secure location with restricted access. This will primarily apply to keys, fobs and contractor access devices. Document and retain records of the destruction of any defective devices.

d. Recover or disable access control devices, upon employee separation from the department or facility. In the event an individual is transferring to another department or location on campus the responsible controller must be notified so access can be changed as necessary. Departments should consult with Human Resources with questions regarding an individual's employment status and or to reissue new access control devices associated with the new work assignment. If an employee is on a long term leave, investigatory leave, or when absence from the campus is for an extended period of time, HR must notify the applicable department manager.

e. Verify annually, in consultation with the applicable Vice President or Dean that those individuals with access control devices remain employed by the University and that their access privileges are current. Routinely verify that access privileges for contractors, guests, vendors or volunteers are still justified for University purposes. If access is no longer warranted for the access control device holder, recover the device(s) and deactivate the access. If the individual has separated from the University, within the week of separation, the supervisor or Chair should notify the applicable controllers to deactivate the access control device.

- Campus Access Control Leaders (CACLs). CACLs are responsible for the administration of access control systems and procedures within their designated areas, in coordination with the Campus Access Control Systems Administrators. The CACLs are designated by the individual in charge of the designated area, which include:

Housing Department – for all residential housing
Security Department – for security department employees and first responders
Facilities Management – coordinates all hardware installation, programming, training and system service.
Computer Services – supports all computing and network services associated with access control systems to include having backup and recovery systems. Manages all programing and software updates.

CACLs, for their designated areas of service shall:

a. Implement access control procedures and secure access control system(s). Security measures used for the access control systems must meet or exceed industry standards including partitioning access control privileges internal to the University; protecting against external unauthorized access; and having redundancy protocols in place.

b. Ensure new Department Access Controllers are trained to perform access control system operations and are familiar with all applicable policies and procedures.

c. Set systems control schedules for operations.

- Facilities Management Department – Security System Technician(s) will assist in providing new Department Access Controllers with formal training on how to utilize the system software to include establishing and/or deactivating access control device privileges within their security partition.

a. Performing and/or coordinating all hardware work on campus managed facilities to include work performed by contractors:

b. Maintaining a master list of all systems installed, the system DAC's established by location and their respective areas of control.

c. Fabricating and duplicating any mechanical keys for all campus managed facilities.

d. Issuing mechanical keys to authorized DAC's for re-issue within their department; obtaining DAC's signatures on key requests and keys issued on Key Request Form; and maintaining and securing records of key transactions in accordance with University policy.

e. Verifying necessary approvals and account codes for mechanical keys and hardware work in accordance with authorized work orders.

f. Maintaining inventory of and securing un-issued mechanical key stock.

g. Coordinating after hours and emergency hardware/key change outs.

h. Providing Access Control Systems training for all newly established DAC's and other personnel as needed. Maintain accurate records of all recorded access control activities. Records shall be archived annually and shall be maintained for three years. All access control records are subject to audit.

i. Ensure relevant emergency access control devices up-to- date to assure timely entry into all buildings by authorized emergency personnel.

j. Add, extend or deactivate authorized access control devices as authorized by the CACL's or DAC's and consistent with this policy. DAC's may activate or change department level authorized access permissions for active access control devices.

k. Document and maintain records of the destruction/recycling of any defective device.

l. Routinely evaluate/test access control systems and requested modifications for functionality and effectiveness. All installations, modifications, repairs and preventive maintenance activities shall comply with University policy and standards. These services must be performed under the direction of the University's Facilities Management department, unless authorized by the Access Control System Administrators.

- Security Measures for System Wide Access

Although all access control devices require care, those assigned system wide access must take extra security measures to secure the device when not in use. System wide access control devices must not leave the University campus unless job functions require otherwise. In no circumstance shall system wide access devices be left unattended or in unlocked vehicles.

- Expiration

Expiration dates may not be displayed on an access control device, however temporary devices have a pre-established date from the time of issuance. Temporary access control devices, including those for contractors, visitors and others will be set for a time period which corresponds with the need of the user.

- Replacement requests

a. In the event of loss, theft or a defective access control device, the assigned device holder shall notify their DAC. A replacement device may be issued in accordance with the department's procedure and this policy. Individuals with access control devices enabled with other functions will also need to notify each service provider to deactivate the functions.

b. The device holder shall take the replacement access control device to his/her DAC for authorization activation in accordance with the DAC's department procedure. The DAC will activate approved access authorizations for the replacement devices and deactivate the lost/stolen/defective device assignments; annotate his/her records with the change; and notify the DAC of the replacement transaction to ensure associated records remain current.

- Changes in Access Requirements due to Change in Status

Departments shall implement procedures to ensure the DAC's are notified when the access requirements for an individual (employee, student, visitor, vendor, contractor, etc.) who has been issued an access control device has changed, such as due to promotions, transfer, separation, or contract expiration.

If the change is due to an individual's transfer to another department:

a. The DAC shall deactivate the department's authorization for access; the new department's DAC may activate the same access control device with the new department's access permissions, as appropriate.

b. If the change is based upon separation from employment, ending a visit to the University, for a contractor whose contract/work is expiring, or the conclusion of the necessity for other temporary use, the DACs shall deactivate the department/facility access permissions and the primary department DAC shall totally deactivate the access control device. The primary department DAC shall take measures to recover the device from an individual who is separating from/leaving the University and destroy access control devices that have an individual's name and image. A record of the destruction shall be retained.

c. DACs shall deactivate generic, short term access control devices issued to individuals whose access permissions are no longer necessary for University purposes or their affiliation has changed. Changes shall be documented.

- Personal Emergency Access to Buildings and Rooms

In case of a personal emergency or inability of an individual to access his/her access control device, the individual must first contact his/her supervisor, department manager, or department access controller to gain access. If unsuccessful, the individual may contact the University security dispatch who will attempt to contact the Security Systems Technician or Locksmith for access. The individual's identity, university affiliation, and access authorization shall be verified prior to granting access.

- Restricted Access Areas

Departments with restricted/high risk areas that require additional access controls, such as specialized labs, shall develop written procedures for controlling access to their restricted areas, in consultation with the applicable DAC, and other university officials as necessary. The procedures shall include:

a. Eligibility requirements for access
b. How to request access
c. Who has authority to approve access
d. Who issues the access control device
e. Who maintains and secures the access control records and unassigned devices
f. How will access control devices be recovered when required
g. Other considerations, as appropriate

Unauthorized locks or access control components will be replaced at the expense of the department and/or college.

VI. FORMS/INSTRUCTIONS (if applicable)

N/A

VII. APPENDICES (if applicable)

N/A

VIII. RELATED POLICIES

- Acceptable Use of Technology Resources Policy
- Personal Credentials Creation and Management Policy
- Email Communication Policy
- Remote Access Management Policy
- Internet Use Policy
- University Network Use Policy

VIV. CONTACT INFORMATION

Campus Access Control Office (CACO) CACO@@aiu.edu.eg

Triggered by:	Name	Date	Sig.
Created by:	Name	Date	Sig.
Revised by:	Name	Date	Sig.
Approved by:	Name	Date	Sig.