MAKERERE UNIVERSITY BIOMETRIC ATTENDANCE MANAGEMENT SYSTEM

(Mak-BAMS)

Biometric Attendance System

GUIDELINES AND PROCEDURES 2024

DESIGN BY ARTHUR MOSES OPIO

Table of Contents

Mak-BAMS

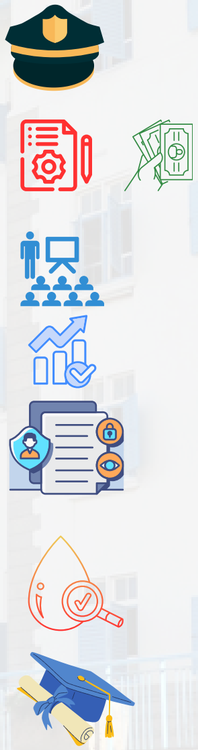
BIOMETRIC ATTENDANCE SYSTEM

GUIDELINES AND PROCEDURES 2024

Introduction

The Makerere Biometric Attendance Management System (Mak-BAMS) has been implemented as a modular component in the Makerere University Physical Identity and Access Management Framework (Mak-PIAM) which aims to address;

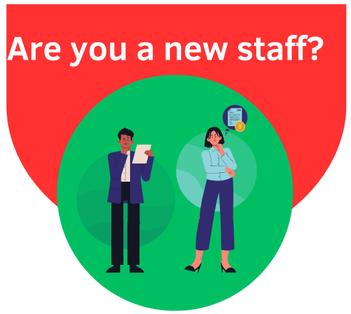
- Security for University Staff, Students, Visitors and properties
- Attendance Management & Payroll Verification for staff
- Lecture Attendance Management for students
- Performance Management for staff
- Secure access to all university electronic resources and Information Systems
- Electronic Quality Assurance (eQA) of both physical and virtual Teaching and Learning
- Graduate Research Supervision



How to Register For Biometric Attendance

A University Staff will;

- Present an appointment letter,
- and a smart/RFID-enabled ID to a Records Officer at the Records and Information Division of the Directorate of Human Resource



You will be required to register for biometric attendance within a ***a period of two weeks*** after receiving their appointment letter.

Mak-BAMS

GUIDELINES AND PROCEDURES 2024

Before applying for a staff-ID

A new staff must:

University Email Address

Create your University email address via https://sso.mak.ac.ug

This **email address** will be embedded within the eHRMS system to enable **initialization** and **access to electronic services** including biometric access amongst others.

Smart Staff ID Application

Log into the eHRMS system https://ehrms.mak.ac.ug and click-on "***ID Requirements***" under the menu on the left pen and read the guidelines for uploading both your ***ID picture*** and ***National ID***.

Visit HR Office

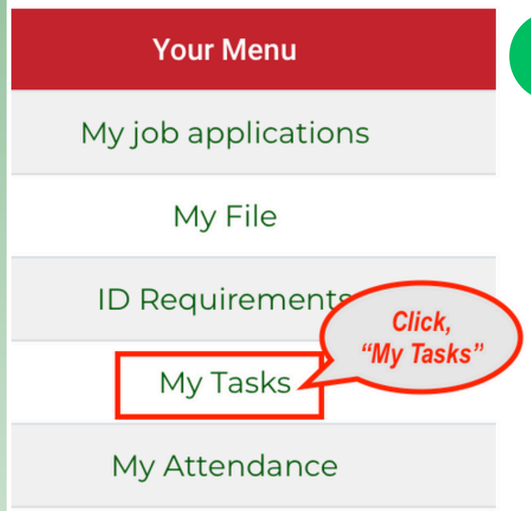
Visit the Directorate of Human Resource for issuance of smart staff-ID after you have submitted requirements.

How to log tasks on the electronic Human Resource(eHRMS)

https://ehrms.mak.ac.ug

Mak-BAMS

All university staff are required to log their weekly/monthly/quarterly or half year tasks on the eHRMS. This includes tasks such as workshops, conferences, seminars etc. scheduled to take place off-campus.



Steps:

- Click ***"My Tasks"*** under the menu on the left pen.
- Click ***"New Task"*** to add a task and its duration.
- You can add as many tasks as you wish.

Upon Submission

Upon submission, **your supervisor** will be **notified** about your logged tasks **via email** and once approved, ***you will not be required to physically clock-in/out for tasks scheduled to take place off-campus.***

Mak-BAMS

Best-user practices for the Biometric Attendance System

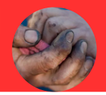
1 No Physical Contact

Minimize physical contact with biometric devices by clocking-in/out using facial recognition.

2 When To Use Fingerprint

Only clock-in/out using your finger-prints in instances where the biometric device is unable to recognize your facial-image

Note: Avoid Fingers that are:

Greasy 

Wet 

Dirty 

3 Seeking Support

Log a ticket via via https://support.mak.ac.ug with subject "**Biometric Failure**" in instances where the biometric device is unable to recognize your finger-prints, facial-image or both

4 Thick Lenses

If you wear glasses with thick lenses, the facial recognition algorithm may struggle to accurately identify your face.

5 Avoid Alcohol Sanitizer

Staff are advised to desist from wetting the devices especially with alcohol-based sanitizers which may affect the devices thumb-print scanner platen (polycarbonate glass-plate where you place your finger-print).

6 Security Audits

DICTS will periodically assess the security and functionality of all biometric devices in the university to ensure optimal performance.

Biometric Data Security and Privacy

The Makerere University Data Security policy broadly classifies university data into Public, Private and Restricted Data. Staff and Student biometric data (finger-prints, facial-images, iris, voice-waves etc.) is classified as restricted-data whose collection, storage, usage and disposal must adhere to a strict set of procedures in order to ensure its Privacy, Integrity and Security.

1 Collection of staff biometric-data

- Biometric data shall be collected by the Records & Information division of the Directorate of Human Resource (DHR).
- Records & division shall only capture staff facial-image and finger-prints biometrics.
- Staff shall sign a “biometric data capture form” consenting to the capture of their personal data.
- Form can be downloaded from https://ehrms.mak.ac.ug

2 Storage of staff biometric-data

- Staff biometric and attendance data shall be stored centrally in a secure & encrypted password protected database.
- User-Access is only available to the attendance data.
- Data Centre entry is restricted to physical security & biometric access.

Mak-BAMS

3 Usage of staff biometric data

- Staff biometric data will strictly be used for attendance management (clocking-in/out).

4 Ethical compliance

Makerere shall not;

- sell, lease, trade, or otherwise profit from staff biometric identifier or information.
- disclose, re-disclose, or otherwise disseminate staff biometric identifier or information unless required by law.
- share personal information; including, but not limited to fingerprint information, with any non-vendor third party organization.

Mak-BAMS

Locations and physical security of biometric devices

The biometric devices are installed in entrance-ways/foyer or reception areas of buildings which makes them accessible and visible to all.

(DICTS) will continuously monitor the up-time/availability of all biometric devices via an electronic console/system and will notify college IT personnel should any biometric device be unavailable

The biometric devices are equipped with a 180-degree view camera that will automatically capture photos of anyone tampering with the device.

Custodians and security personnel of university premises as well as IT personnel at user-units (colleges), are required to ensure the physical security of biometric devices at their units.

The biometric devices are tamper-proofed with an alarm system which will be triggered in the event that the device is forcefully tampered with.

The security office of the university will ensure the security of all biometric devices installed at the main-gate, western-gate and eastern-gates of the university.

End-user support guidelines

Mak-BAMS

1ST LINE TECHNICAL SUPPORT

If the biometric device at your user-unit is not powered, report the incident to your college IT personnel. This may be a local power-related issue that the user-unit IT personnel can resolve. If all fails, they will log a ticket via https://support.mak.ac.ug and escalate the inquiry to DICTS.

2ND LINE TECHNICAL SUPPORT

If the biometric device is unable to recognize your facial-image, finger-prints or both, first refer to the best-user best practices for the biometric attendance system for guidance. If all fails log a ticket via https://support.mak.ac.ug for DICTS to address your inquiry.

3RD LINE TECHNICAL SUPPORT

In the event that the biometric hardware or software fails, DICTS will contact the manufacturer for support. In such circumstances, staff will be advised to clock-in/out from any device they can access including those at university gates as they await repair of device(s) for their premises.