APPENDIX 1: TECHNICAL SPECIFICATIONS AND REQUIREMENT
INTEGRATED ASSET & SECURITY MANAGEMENT SYSTEMS
INCLUDING SECURITY TURNSTILES AND IT’S RELATED SERVICES
FOR MIMOS BERHAD

A. SYSTEM REQUIREMENT

Functional Requirement

1. Asset Management Module that capable to perform, at minimum, the following tasks:
   a. Real-time tracking and locating of assets within MIMOS’ predefined labs or departments or areas within MIMOS premises
   b. Real-time visibility of mobile and high value assets with real time tracking, monitoring and security features
   c. Automated asset auditing and stock count
   d. Automated and real-time reporting of asset movement and locations
   e. Automated recording of assets taken out through the exit (6) doors
   f. Automated alert and notification system on unauthorized asset movement or status.

2. Security Access Management System must be able to perform multiple functions and integration of security features in MIMOS which include:
   a. door access management (biometric and non-biometric readers/controllers),
   b. Turnstiles (waist-height and full height)
   c. Other Security barriers (which include boom gates, swing door etc)
   d. Biometric TMS reader/ time clocking,
   e. Guard Tour Tracking & Reporting Subsystem
   f. Intrusion Monitoring
   g. ID/Badge Printing software to "Peclin" Printer
   h. Visitor Management sub-system
   i. CCTV Interfacing Sub-system (existing)
   j. Interfacing with Fire Alarm System (existing)
   k. Sms alert

Existing Door Access Points/Readers and TMS Readers

<table>
<thead>
<tr>
<th>Door Access Reader cum Controller</th>
<th>Biometric TMS Reader cum Controller</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology Park Malaysia (TPM)</td>
<td>Technology Park Malaysia (TPM)</td>
</tr>
<tr>
<td>Kulim Hi Tech Park (KHTP)</td>
<td>Kulim Hi Tech Park (KHTP)</td>
</tr>
<tr>
<td>Total</td>
<td>Total</td>
</tr>
<tr>
<td>CES</td>
<td>1</td>
</tr>
<tr>
<td>ECARD</td>
<td>113</td>
</tr>
<tr>
<td>EJARI</td>
<td>12</td>
</tr>
<tr>
<td>SMART READER</td>
<td></td>
</tr>
<tr>
<td>TOTAL</td>
<td>126</td>
</tr>
<tr>
<td></td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>136</td>
</tr>
<tr>
<td></td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>12</td>
</tr>
</tbody>
</table>
APPENDIX 1: Technical Specifications & Requirement

Required Turnstiles Types and Location

<table>
<thead>
<tr>
<th>Type</th>
<th>Location</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 lanes bi-directional waist height</td>
<td>Main Lobby</td>
<td>2</td>
</tr>
<tr>
<td>1 lane bi-directional</td>
<td>4 locations in TPM</td>
<td>6</td>
</tr>
</tbody>
</table>

Existing CCTV System: 1) DVR Panasonic and 2. NVR Indigo System

2. The software should provide user friendly features to provide proper access control, time management system, visitor management system and ID/card management system and unified user interface with GUI that include floor plan and location of doors and CCTV with proper licenses that link and allow sharing of data between MIMOS at TPM Kuala Lumpur and MIMOS in KHTP, Kulim, Kedah.

3. All hardware – computers, readers/controllers and barriers & turnstile readers - must be able to communicate via industry standard TCP/IP protocols

4. The desired system is shown in architectural diagram below.

Proposed MIMOS Integrated Assets & Security Management System Architecture Diagram

- The systems must be able to interface with Corporate Human Resource (CHR) SAP data base for the provision of effective clock in/out data to CHR/Employee Self Service (ESS) Absent & Leave Report
APPENDIX 1: Technical Specifications & Requirement

b. The system must be able to provide visitor management capabilities which include reading input from Malaysians MyKad, and Passport and other substitute documents for foreign visitors, issue and retain visitor pass/card at the turnstiles

c. The system must be able to integrate the CCTV surveillance solutions from Panasonic DVR and Indigo NVR and direct from the desired cameras locations

d. The system must be able to support future need to “alert” and “report” assets tagged with RID passing through main exit doors.

e. The systems must be able to provide single unified user interface for monitoring and control of access, intrusion and CCTV/digital video solutions.

f. The systems must be able to provide web based alert solutions for assets and security intrusion

g. The system shall have a user friendly features at the System Administration Workstation, Visitor Management Workstation and Operations Control Centre (OCC)

5. The Security Management Systems (of the project) is required to replace the present door access management systems but it must be able to use the existing Mifare smart card IDs, the door access readers cum controllers and the related infrastructure (power, network connection and locking devices)

6. To be deployed at both MIMOS TPM and MIMOS KHTP and the system shall be deployed on a network; it shall be based upon a TCP/IP 10/100/1000 architecture.
B. SPECIFIC REQUIREMENT

1. ASSET MANAGEMENT SYSTEM
   a. The basic system of asset management module must have an open system architecture, support Oracle and Microsoft SQL Server databases, cover current interface standards and support at least the following basic functions:
      o Asset Tag – Active RFID with smart sensors which will be embedded into assets and equipment for real time wireless traceability and monitoring
      o Active Reader – Hardware which will read and relay the received information from the asset tags to the enterprise software
      o Cabling and Networking – CAT5E connectivity and networking from Active Readers to the Server
   b. The basic system for the implementation of asset management is as follows:
      o Active Readers are mounted in work areas and defined as locations such as Finance Dept, Engineering Lab – MEMS or IT Dept. These readers will scan and receive signals from Active RFID tags embedded in assets and equipment.
      o When mobile assets pass through the defined zones, the Asset Tags will communicate with the Active Readers.
      o The received signals and data packets will be processed by the Active Readers and relayed to the Server for the Enterprise software to process. The logical layer of the software will then determine if certain actions need to be executed, or if certain rules or logics have been breached so notifications need to be sent.
      o The full history of the assets movement and location within the building can be recorded, monitored and filtered according to user’s requirements.
      o At any given time, users may login and perform exercises to:
        i. Search a particular asset’s location
        ii. Summarize the total number of assets in the building, and its respective location
        iii. Apply rules and triggers so a particular asset is not allowed to leave or move from a defined area
        iv. Apply real time notification via email or SMS to notify stakeholders if a certain breach has occurred.
c. Specification of Components for Asset Tagging

i. Asset Tag

The Active RFID tag with smart sensors is a high performance wireless transceiver device which can be affixed to virtually any asset or equipment (laptops, computers, laboratory / electronic equipment, pallets, inventory items, etc.). These devices transmit and receive signals and information pertaining to the location, status and ID of the tagged asset or equipment.

Signals from an Active RFID tag can travel and be detected from much farther distances up to 150m in a line of sight situation. In an office environment, its signal can penetrate through doors, walls and other obstructions such as cubicles and cabinets. This feature allows it to appear ‘visible’ in the system at all times.

The general specifications of the Active RFID tags are:
- Functional on 2.4Ghz or 433Mhz frequency with embedded microprocessor and firmware, with built in motion sensors
- Ultra Low Power architecture with 3 years usage with single CR2032 coin battery
- Covering at least 150m range
- Slim fit enough to be applied on or within an asset or equipment

ii. Employee Tag (Not for immediate implementation)

The Employee Active RFID tag provides convenient, hands free identification of personnel for access control and people tracking without getting close/touching the reader or transponder. Tag signals can travel longer distances than the normal passive/proximity employee cards for more than just employee tagging, but also security and movement / access controls.

The general specifications of the Active RFID tags are:
- Functional on 2.4Ghz or 433Mhz frequency with embedded microprocessor and firmware, with built in motion sensors
- Ultra Low Power architecture with 3 years usage with single CR2032 coin battery
- Ability to be detected from within a bag or pocket, allowing an automated presence verification at any door access

iii. Active Tag Reader / Sensor

The Active RFID Tag Reader or sensor is a networked transceiver device which can detect signals from the Active RFID tags, and convert them into data to the application software.

The Active RFID Reader will be networked via CaT5E lines to the application server where data will be passed to the application engine for processing and aggregation.

The general specifications of the Active RFID reader are:
- Functions on 2.4Ghz or 433Mhz RF
APPENDIX 1: Technical Specifications & Requirement

- Ability to read and process hundreds of Active RFID tags simultaneously
- Real time data push to server for software processing and data aggregation

iv. Multi Tier Enterprise Application
- The central software system to monitor the tagging, tracking and monitoring of assets within the building
- Web based software for ease of deployment and usage by respective MIMOS users
- Open and scalable using basic common software development languages (such as .Net, PHP, Flex and mySQL) for easy customization and future enhancement
- Built in reporting module to ease data aggregation and dissemination
- Built notification services and features for integration with email, SMS or other alert systems preferred by MIMOS
APPENDIX 1: Technical Specifications & Requirement

2. SECURITY ACCESS MANAGEMENT SYSTEM

2.1 GENERAL

The requirement for the Security Access Management Systems:

- The system must be able to perform multiple functions and integration of security features in MIMOS which include door access management (biometric and non-biometric), barriers (which include turnstiles, boom gates, swing door etc), time clocking, intrusion monitoring and guard tour.
- The systems must be able to interface with Corporate Human Resource (CHR) SAP data base for the provision of effective clock in/out data to CHR/Employee Self Service (ESS) Absent & Leave Report.
- The system must be able to provide visitor management capabilities which include reading input from Malaysians MyKad, and Passport and other substitute documents for foreign visitors, issue and reads retained visitor pass card at the turnstiles.
- The system must be able to integrate the CCTV surveillance solutions from Panasonic DVR and Indigo NVR and direct from the desired cameras locations.
- The system must be able to receive “alert” signals and “report” Rfid tagged assets that passed through exit doors.
- The systems must be able to provide single unified user interface for monitoring and controlling of access, intrusion and CCTV/digital video solutions.
- The systems must be able to provide web based alert solutions for assets and security intrusion.
- The system shall have a user friendly GUI features at the Asset Management Terminals, System Administration Workstation, Visitor Management Workstation and Operations Control Centre (OCC).

i. For the Security Admin Workstation, the software should provide user friendly features for the registration of new staff and automatic creation and printing of photo ID; deregistration of staff but keeping the staff particulars, suspension and blacklisting; time zoning and locking plan management, plus access management report which include the capability to provide the number of people in the building at any time on demand.

ii. The workstation at OCC should be provided with unified view of floor plan of access points, CCTV and real time CCTV data and recorded view.

iii. The visitor management system should have the feature to issue restricted or zone visitor card and retain the card in the turnstiles at the end of the visit.

iv. For web-based alert, the system must be able to generate and send alert to laptop and hand held devices via sms and email.

- To be deployed at both MIMOS TPM and MIMOS KHTP and the system shall be deployed on a network; it shall be based upon a TCP/IP 10/100/1000 architecture.
2.2 DOOR ACCESS

For the Security Admin Workstation, the software should provide user friendly features for:

a. the registration of new staff and send staff information for ID/batch with photo printing at the printer
b. sufficient/customized fields for staff information
c. deregistration of staff but keeping the staff particulars,
d. suspension and blacklisting of staff/visitors;
e. time zoning and area zoning
f. locking plan management,
g. linking with the turnstiles and provide access management report and function to provide the number of people in the building at any time
h. keeping and allowing fast retrieval of an individual (employee or any ID holder) historical access activities
i. keeping and allowing fast retrieval of access door readers activities
j. real time report/record of access door performance
k. reading/retrieving records of specific door and all doors performance – uptime/down time
l. must be able to interface with MIMOS Firealarm system and release all doors when fire alarm is triggered or released.

2.3 TIME MANAGEMENT

The system must be able to provide at least the following requirements:

a. The readers and the software must be able to read finger print/biometric inputs in less than 3 seconds
b. The system must be able to identify the first (in) and the last record (out) reading of the day for every employee
c. Clock In/Out data must be efficiently sent to CHRSS Absent and Leave Records
d. Easy features/command to read and print historical records for every employee
e. Friendly function/button to click on to get the number of people clock in and out for the day and past days’ records.

2.4 SUB SYSTEMS

2.4.1 VISITOR MANAGEMENT SYSTEM (VMS) AND INTEGRATION

The VMS subsystem must have at least the following features:

a. The system must be linked and integrated with turnstiles and access readers
b. VMS workstations are equipped with the peripherals to read MyKad and other substitutes for foreign visitors
c. The VMS terminal/workstation efficiently issues pass for restricted zones and/or unescorted visitors
d. Workstation records visitors card returned/retained in the turnstiles
e. Database management of all historical records for blacklist verification and automatic update for repeat visitors
f. Friendly quick functions to check number of visitors in the building, and daily record on number of visitors
g. Visitor web-based pre-registration function (optional)
2.4.2 ID/Photo Printing Requirement
ID/photo badging or card issuing management system with the following function:
   a. Link ID/badge printing machine to Access Management Workstation
   b. Print badges by capturing personal information and ID particulars from the access management database
   c. Have ID/photo database (photos and personal particulars) for reprint of ID/badge
   d. Can capture image from any video camera or scanners
   e. The software are supported by most of the graphic formats. (E.g. BMO, PEG, Tiff, GIF. etc)

2.4.3 DVR/NVR Integration to Security Access Floor Plan
The system must have the following features:
   a. Click on camera icon for live video display or camera control
   b. Event triggered video recording and playback by clicking camera icon
   c. Automatic live video pop-up on alarm trigger
   d. Search recorded video for playback

2.4.4 Easy To Monitor Graphical User Interface (GUI)
The system must be able to provide easy to observe and use GUI for intrusion detection, access control and CCTV with floor plan and camera and access door locations. This will include:
   a. The capability to give automatic live video window pop up upon alarm activation or clicking the respective cameras
   b. To display/alert doors that are opened for more than certain time (3 minutes)
   c. Access control device parameters linked to CCTV cameras

3. The basic system of an security access management system must have an open system architecture, support Oracle and Microsoft SQL Server databases, cover current interface standards and support at least the following basic functions:
   - Freely scalable system solution, i.e. expandability must be guaranteed over the entire life cycle with full upwards compatibility (life cycle management or LCM) It must be possible to implement the organisational and technical security requirements in a flexible, modular manner
   - Open system architecture, i.e. the use of existing IT infrastructures and IT environments must be possible. Oracle and Microsoft SQL Server databases must be supported. See also System Architecture
   - The system solution guarantees distributed intelligence with a decentralized architecture to ensure maximum operational reliability and stability.
APPENDIX 1: Technical Specifications & Requirement

- The basic system must include all necessary management, alarm and logging functions.
- Support of Single Sign On (SSO)
- Staff data management: Registration and management of staff data, including photo. Assignment of access rights and time and attendance (T&A) models. Generation and detailed evaluation of reports and statistics based on defined criteria.
- System management: Central configuration and management of peripheral devices in the system. It must be possible to use the same system management for both online and standalone components, in other words non-wired access points.
- Management of mechanical locking systems of 50 components
- Logging: Recording of all events, alarms, instances of access, system errors, security-related user actions, etc. must be guaranteed at all times in both online and offline mode.
- Monitoring and control of various alarm zones in connection with an intruder detection system.
- It must be possible to transfer the access rights and T&A data from an active badge to a transition badge if required
- It must be possible for remote maintenance to establish a connection between headquarters and a remote branch office over a phone line.
GENERAL SYSTEM REQUIREMENT

1. System Architecture
   a. Operating Systems
      The System shall function under the latest/any Windows platform:
      i. Vista Enterprise
      ii. Vista Ultimate
      iii. Vista Business
      iv. XP Pro
      v. Windows 2003 Server

   b. Server/Client
      Any server/client running operating systems listed in 1a above will be capable of
      running both the Client and Server Software. The server/client shall have a
      standard 10/100/1000 Ethernet Card.

   c. Network Requirements
      The system shall be deployed on existing MIMOS network infrastructure; it shall
      be based upon a TCP/IP 10/100/1000 architecture.

   d. System Structure
      The System shall consist of 3 sections
      i. Server Software
         The Server Software shall consist of the database, communications protocol
         to the access control hardware, communications protocol to the Clients and
         a GUI for Server administration. Because of security concerns, the sole
         method for accessing the Server shall be the Client. There shall be no
         browser access into the Server. The complete Software database shall
         reside solely on the PC housing the Server to take advantage of network
         back up tools. The complete Server Software and Database shall not reside
         solely on the access control hardware. The database shall be SQL
         compliant. There shall be no 3rd party license fees associated with the SQL
         database.

      ii. Client Software
         The Client (defined here as the application/Client by which users interface to
         the system: it has no processing or database storage functionality) shall
         provide the sole means of controlling the access control hardware via the
         Server or making changes to the Server database or reporting on system
         activities. There shall be no browser interface to the system to minimize
         security risks. The Client may be installed either on the same PC as the
         Server Software or a different PC.

      iii. Security Access Control Hardware
         The security access control hardware shall have the capability to control and
         monitor all doors (turnstiles, boom gates etc), exit devices, locking
         hardware, Readers and security detectors.
2. Hardware (Field Devices) For Security Door Access

a. Scope of Control
The vendor shall be able to integrate and utilise the existing Neural access reader cum controller as per the specification outlined below:

b. Capacity
The limit on the number of doors shall be solely constrained by Ethernet and TCP/IP standards

c. Communication
i. Communication to Server
   All communication to the Server shall be via a TCP/IP 10/100/1000 bus.

ii. Communication between Reader cum Controller
   1. Supported Network Type
      The Reader cum Controller shall have Ethernet hardware and TCP/IP protocols embedded built in, without requiring additional boards or converters. All communications between Reader cum Controller shall be via a TCP/IP 10/100/1000 bus. The Readers cum Controllers shall operate on a true Peer-To-Peer protocol with each Reader cum Controller being able to communicate directly to other Readers cum Controllers and to the Server. There shall be no single point of failure within the Security Access Control hardware where communication or decision making is compromised. There shall be no master-slave architecture.

iii. Response Time
      On a dedicated TCP/IP network without other network traffic, the response time between inputs and outputs on different Controllers shall not exceed 1 second communication between other Controllers and the Server.

d. Reader cum Controller Interface
   i. Reader Cum Controller Types and Formats
      Vendor shall be able to integrate with Neural reader cum controller format as per the specifications provided.

( Kindly refer to Appendix 2 for matters related to existing items, d to j )

e. Reader cum Controller Memory
   i. Memory Type
      The Existing Reader cum Controller's memory is non-volatile (supported by a lithium battery) with an expected life of 5 years. The Reader cum Controller will send a notification to the Server Software when the lithium
battery power approaches a state where it can longer back up the memory.

ii. Reader Cum Controller Cardholders Storage

Refer to Appendix 2

iii. Events

The Controller shall store up to 10,000 events should communication fail between it and the Server. The system will automatically send events to the Server during normal communication. The Controller shall be configurable such that only events designated by a system administrator are stored. Should the event buffer become full, each Controller will delete events only as needed on a first in, first out basis. Each Controller’s memory shall operate independently of all other Controllers.

f. Surge Protection
   i. Power Protection
      The Controller and Expansion modules shall be protected by a self-resetting, thermal fuse as well as diode protection. The Reader shall have reverse voltage diode protection.

   ii. Network Protection
      The RS-485 network shall be protected by diodes and gas discharge tubes on all communication ports.

   iii. Input Protection
      All inputs shall be protected against power surges by diodes.

   iv. Output Protection
      All outputs shall be protected against power surges by MOVs and resistor snubber circuits.

   g. Power Requirements
      i. Reader cum Controller
      The Reader cum Controller shall be powered from 12VDC and draw no more than 650mA at 12VDC when all outputs LEDs and communication buses are fully active.

h. Indicators
   i. Communication Buses
      1. There shall be LED indicators for RS-485 network activity
      2. All TCP/IP networking lines shall have LEDs to indicate network speed and activity (10 or 100 mb),

   ii. There shall be a power fault LED for over voltage and backwards voltage.
iii. There shall be a reset LED to indicate when the Controller memory is cleared.

iv. All relays shall have status LEDs indicating their programmed logical status.

i. Operating Temperature
The operating temperature range of the Controller shall be no less than
-40º F to 140º F (-40º C to 60º C) at 0% to 90% Relative Humidity, non-condensing.

j. Connections
   i. Power, and RJ 45 connection
      These shall be made via quick disconnect connectors. TCP/IP connections shall be made with an RJ-45 connector or optionally with the quick disconnect connector also provided on the Controller.

3. Cards and Tags
MIMOS existing Mifare/smart card to be utilized. Format as follows:
   a. ISO Card
      The Card shall be capable of accepting a direct print of photo and other graphics from a dye-sublimation printer.
      Mifare card technology with 13.56Mhz
      The dimension shall be 3.38” x 2.13” wide x 0.031” thick (86 mm x 54 mm x 0.08mm).
      The color shall be white with the encoded number and a date code printed on its surface.

4. Security Access Software
   a. Configuration
      All configuration, programming, and monitoring of the Security Access control system must be done through a Client Software program that makes these tasks easy to perform and is supported training. For security purposes, no browser-based software configuration shall be acceptable.

   b. Features
      i. The Software shall be a Client-Server architecture with no browser access into the system to minimize security concerns.

      ii. Multiple Operators (minimum 2 operators/terminals) shall have the ability to concurrently connect to the access control Server.

      iii. The system shall have the ability to be divided into an unlimited number of sites up to the number of readers in the system.
iv. The system will allow system operators to be assigned different privilege levels at different sites.

v. The system will allow the user to create an unlimited number of user definable fields in the cardholder record.

vi. The system will allow for different daylight savings time schedules based upon a Controller’s location.

vii. All relay points must be optionally programmable to either follow the state of an associated input point, to be latched to a state based on an input point or formed a specific time period after being triggered by an input state.

viii. All input monitoring points must be linkable to output relay points, allowing input events to initiate output relay responses.

ix. For each Reader cum Controller and its associated I/O Expansion Boards, if any, all input monitoring points and output relay points on that Reader & Controller must be able to be used in multiple links on that Controller, allowing any combination of Reader cum Controller inputs to trigger any combination of Reader cum Controller outputs.

x. An unlimited number of access groups (combinations of access/egress points and time zones) shall be available for creation and assignment of Cardholders access privileges.

xi. Cardholders can be assigned to an unlimited number of access groups.

xii. The Software shall contain a utility to automatically store archived event data in weekly, monthly or yearly files.

xiii. The Software shall have the ability to optionally configure up to three, separately configurable, event monitoring windows, with each window capable of displaying operator-selectable event information.

xiv. It shall have the ability to automatically unlock and relock specific doors at specified times of the day and day of the week, with user-defined overrides on user defined dates.

xv. The Software shall have the ability to disable the reporting of specified events that do not need to be tracked, to save event storage space on the Controller.

xvi. The Software shall have the ability to poll the access control network and retrieve network hardware status information that the program uses to automatically setup and configure itself without manual data entry.

xvii. It shall allow the assignment of future activation and expiration dates and times to individual Cardholders, which are stored at the Controller level.
operator shall be able to set the time frame for activation or deactivation in 1 minute increments.

xviii. It will allow multiple Access Groups per Card user.

xix. The Software will allow multiple Credentials per user.

xx. Readers cum Controllers may be assigned to local geographic time zones so the system can accurately report local times for events.

xxi. The system will allow the customer to design various action sequences using the Reader cum Controller’s inputs and outputs to allow for user defined needs.

xxii. The system shall allow manual or automatic assigning of static Ethernet addresses.

xxiii. The system shall be capable of accepting future activation or expiration dates for users. The system operator shall have the capability to enroll such time periods down to the minute on any calendar day. These dates shall be kept in the Reader cum Controller rather than downloaded from the PC.

xxiv. The Software shall automatically find and configure in its database all Reader cum Controllers, Expansion boards (if applicable), Interface boards and Readers attached to the system.

xxv. The Software will automatically assign Static IP addresses to the Controllers based on starting IP address provided to the Software.

c. Capacities
   i. There shall be an unlimited number of operators capable of configuring, monitoring, and operating the system.

   ii. The Software shall have the ability to manage up to 64 distinct time zones with each time zone subdivided into the 7 days of the week divided into 4 start/stop time intervals and 6 holiday schedules.

d. Reporting
   The Software shall have a library of pre-defined, commonly used reports, and will also allow for the use of 3rd party reporting tools for user-generated custom reports.

e. The Security Access Software shall be able if not defined earlier to perform the following:

   i. People in the premises at any given time
      • Head count or the number of people in the building at any given time (people coming in through the turnstile and out through the turnstile);
The number of people can be broken down according to group of ID or card holders (employees, third party employees, contractor, visitors and etc);

ii. Report
Turnstiles - Activity report (in and out) at specific and all the turnstiles

iii. Security Access & Controller Uptime Report
Daily report, weekly and monthly report on any security access door that are not performing.

iv. The Security Access Software should have the following functions or modules as the part and parcel of its basic capabilities:

- Control the operations of access doors that are required Mifare Card alone or Mifare card and biometric (finger) as identities. Access doors include doors, turnstiles, boomgate and etc.;

- Time management /Clocking in and out function whereby “staff clock in/out” at the reader cum controller using ID and fingerprint identities are seamlessly captured and efficiently transferred to MIMOS staff absence and leave report in Employee Selfhelp System (ESS) riding on Human Resource application using SAP platform;

- Intrusion Reporting due to attempts to force entry through the access doors (specifically at doors and turnstiles)
- Tour Guard functionalities and reporting;
- The software shall be able to interface with MIMOS Firealarm System for the purpose to release all door under emergency triggers

v. The Security Access Software shall have or compatible with the following additional modules:
- Visitor Management System (VMS)
- Floor plan for CCTV and access door surveillance
- SMS/Alert requirement
- Receiving alert from the transponder of the Asset Security Management System
3. TURNSTILES

3.1 General Requirement

a. The required turnstiles is motorised device with sensor monitored lane or passageway to control and record pedestrian entering or exit from MIMOS premises through predetermined exit points or doors.
b. The height of the turnstile is waist height or half height with two swing barrier panels made of polycarbonate
c. The half-height turnstile mechanism (sensor and motorised features) must be able to work with Security Access Management System that uses Mifare card to carry the identification of the authorised person to enter and exit MIMOS premises.
d. The turnstiles must be smart enough to allow bi-directional passage by displaying the indicative light for entry or exit mode.
e. The swing barrier panels would open the passage upon receiving the positive identification from the access reader cum controller installed at the barrier.

3.2 Structure

a. Guiding elements and handrail are made of stainless steel AISI 304 / V2A (1.4301).
b. Guiding tube and card reader post are to be stainless steel posts Ø 140 mm and 6 mm thick.
c. In fill panels are 10 mm toughened glass panels.
d. Housing of the drive system and controller are made of stainless steel AISI 304 / V2A (1.4301)
e. Stainless steel satin finish, grain 320
f. Two swing barrier panels made of transparent polycarbonate, 10 mm thick with upper edge 1,000 mm high.

3.3 Sensor

a. The sensor system should be integrated in the respective handrail
b. The entrance sector must be monitored by the sensor system.
c. The rotation angle of the barrier elements must be monitored by the sensor system providing a protective safety area.
d. The sensor system must provide a single passage regulation in both directions. It must provide:
   - easy passage, even with bags or luggage
   - safe passage with no contact with swing panel
   - high throughput rate and high pedestrian safety

3.4 Drive System

a. The drive system must be a low energy drive with an adjustable speed.
b. It must have a smooth operation with guaranties a long life time.
c. The speed and position must be controlled by incremental decoder without the need for mechanical switches (latest technology.)
d. There should be an integrated friction brake, to protect a mechanical damage of drive.
3.5 Performance

a. The half-height turnstile shall be able to support a throughput of 30 to 60 people per minute, depending on the security access control.
b. The parameters may be adjusted on site:
   - opening or closing time
   - audible and visual alarm, in seconds
   - the time the barrier will wait for a person to enter the lane after a card is presented
   - the length of time to allow a beam to be blocked before generating an alarm
   - whether to generate an alarm when a person partially enters then backs out
   - a confirmation signal when a person walks through a lane in “Open Mode”
c. The turnstile must provide alarm outputs for the following:
   - Intrusion - a person is detected in the lane without a valid card
   - Tailgating - one or several persons follows illegally behind another user
   - Opposite direction - when the barrier opens, a person enters from the wrong direction
   - Equipment fault

3.6 Operation Mode

a. The turnstile must provide bi-directional access control.
b. The following operation modes must be possible:
   - Open Mode - Basic position open: without authorization door wings close automatically.
   - Closed Mode - Basic position closed: authorized person – door wings open automatically in passage direction and close then again.

3.7 Displays

a. Orientation displays must be provided.
b. The displays should be mounted in the Ø 140 mm guiding tube.
c. The card reader must be integrated with the signal display (red / green).
d. The display shall be show red or green to indicate the turnstile status.
e. Upon acceptance of a valid “GO” signal from the security access control system, the green lamp lights to indicate that mechanism is unlocked and passage is permitted.

3.8 Card Reader Posts & Visitor Collecting Box (if required)

a. The card reader must be integrated with card reader and signal display.
b. There must be a card slot and lockable collecting box built in to the post to receive visitor cards.
c. There must be a tray for returning non-readable or invalid cards.
d. It should be possible to identify the presence identification of non-readable cards.
e. The card reader posts & visitor card collecting box must be integrated into the lane.
3.9 Control Panel

a. The turnstile must be controlled remotely via control panel located behind the security counter. The following functions should be provided:
   - Single release entry / exit
   - Day / Night Operation (Open / Close Mode)
   - Block
   - Permanent release Entry / Exit

3.10 Technical Requirement

a. Electrical power supply: 230V single-phase, 50 Hz
b. Power consumption at rest = 120W per walkway
b. Power consumption in operation = 250W per walkway
c. Life cycle 1 200 000 – 3 000 000 switching cycles
d. Locking torque for toothed holding brake ≥120 Nm
e. Max. drive torque 5 Nm

3.11 Dimensions (Adjust according to specific site and model required)

a. Passage width = 650 mm
b. Total width = 1,060 mm
c. Height of the interlock = 1,000 mm
d. Length of the interlock = 1,760 mm
e. Height of barrier panels = 1,000 mm

3.12 Environmental Data

a. The turnstile shall operate satisfactorily under temperatures comprised between -20° to +55°C.
b. The turnstile shall have optimal functioning to up to 95% humidity.

3.13 Certifications

a. The turnstile can be manufactured according to “CE” standard (European).
b. The supplier must be certified ISO 9001 by an independent auditing instance.

3.14 Experience

a. The turnstile shall be of proven design and the manufacturer must have at least 10 years documented experience in this field
b. The turnstiles must have local expertise technicians/engineers to oversees its installation and maintenance
c. The vendor must show proof of model projects or organisation utilising satisfactorily the turnstiles
APPENDIX 1: Technical Specifications & Requirement

TURNSTILES SPECIFIC REQUIREMENT

1. **Main Lobby**
   1.1 Format 1 (1760mm x 1020mm) with base cover plate and 140mmØ post
   - Interlock length 1760mm; Interlock height 1020mm
   - Passage 650mm
   - Passage width = 650mm
   - Guiding elements made of stainless steel AISI 304 Ø 60mm with 10mm toughened glass panels and AISI 304 stainless steel handle
   - Integrated sensor system in respective handrail
   - Type 2 power assisted motion:
     - 2 servo-positioning drives / 2 directions electrically controlled, drives
     - Entrance sector monitored by simple sensor system in compact overall length (ground regulation in both directions, Security Level 1)
   - 2 operation modes
   - Signal Device LED Green "=>" and Red "X" included

   1.2 Location: 2

   1.3 No of single unit: 2
   1.4 No of extension unit: 2
   1.5 No of manual swing glass door between the turnstiles: 1
   1.6 Glass wall to cover gaps between turnstiles and the premises walls
   1.7 Installation: cover engineering, electrical and network

2. **Lift lobby**
   2.1 Format 2 (1660m x 945mm) come with base cover and 140mmØ post
   - Passage width = 650mm, Total width = 1060mm
   - Interlock height 945mm, Interlock length = 1660mm
   - Guiding elements made of stainless steel AISI 304 Ø 60mm with 10mm toughened glass panels and AISI 304 stainless steel handle
   - Integrated sensor system in respective handrail
   - L = 1660mm / W = 130mm / H = 45mm
   - Door wings made of transparent polycarbonate, 10mm thick, upper edge 900mm
   - **Type 2 power assisted motion:**
     - 2 servo-positioning drives / 2 directions electrically controlled, drives
     - integrated in the housings
     - Entrance sector monitored by simple sensor system in compact overall length (ground level of single passage regulation in both directions, Security Level 1)
   - 2 operation modes

   2.2 Location: 1
   2.3 No of single unit: 1
   2.4 No of door access reader cum controller: 2
   2.5 Installation: cover engineering, electrical and network
3. **West Entrance**
   3.1 Format 2 with 140mmØ post
   Specifications same as lift lobby
   3.2 Location: 2
   3.3 No of single unit: 2
   3.4 Glass wall and door between the 2 units
   3.5 No of door access cum readers: 4
   3.6 Installation: cover engineering, electrical and network

4. **East Entrance**
   4.1 Format 2 with 140mmØ post
   Specifications same as lift lobby
   4.2 Location: 2
   4.3 No of single unit: 2
   4.4 Glass wall and door between the 2 units
   4.5 No of door access cum readers: 4
   4.6 Installation: cover engineering, electrical and network

5. **Wafer Fab**
   4.1 Format 2 with 140mmØ post
   Specifications same as lift lobby
   4.2 Location: 1
   4.3 No of single unit: 1
   4.4 Glass wall and appropriate structure to cover gaps between turnstile and premises walls
   4.5 No of door access cum readers: 2
   4.6 Installation: cover engineering, electrical and network
OTHER REQUIREMENT

1. WARRANTIES
   The product warranty to the user warrants the software, hardware, equipment and turnstiles to be free from defects in material and workmanship for the following time period from the date of purchase.

   1.1 Half-height turnstiles
      a. Sensor and mechanical/motor
         A two-year no questions asked warranty for these components
      b. Structural defect
         A limited lifetime warranty

   1.2 Asset RfID Reader
      a. A limited lifetime warranty of the active tag life span

   1.3 Active RfID Tag
      a. A limited lifetime warranty as per declared active tag life span

   1.4 Software Functionality and Interfacing Capability
      a. A three-year no questions asked warranty

   1.5 Others
      To list specific items and defined the warranty terms and duration/year under warranty

2. DOCUMENTATIONS

   2.1 Vendor to list the operations manual for the systems and products provided as per this project