اللجنة العليا
للمشاريع والإرث
Supreme Committee
for Delivery & Legacy

Business Requirements Specification

UNISTAD
Al-Janoub Stadium
Integrated Building Management Services

Prepared for: Supreme Committee for Delivery & Legacy

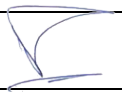
Document Reference number: SC-I60-CAB-ORD-SPE-IT-00015

Prepared by: Ooredoo

Supreme Committee for Delivery & Legacy
PO BOX 62022, Al Bidda Tower, 34th Floor
Corniche Street, Dafna Area, Doha, Qatar

Approval sheet

Document owner: Muhammad Abdullah Rana

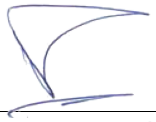
Signature: 	Date: 29/11/2020

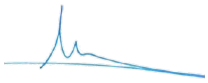
UNISTAD WO ref. number: WO-03 (WK.DG1) - 20181022

Revision history

Revision	Date	Additions/modifications
0	22-Oct-18	First issue
1	17-Dec-18	Document format has been updated and standardised to also include stakeholder against the requirements. The relevant stakeholders have been included.
2	14-June-20	The requirements modified/ removed for ACS and CCTV since they will be covered in respective BRS or not in the IBMS scope. Refer Section 3 for details.
3	29-Nov-20	The stadium BRS for the IBMS Service is already approved by the business stakeholders for the functional scope and the requirements. This revision only constitutes newly added the Green Stadium requirements pertaining to the stadium in section 1.4.1.9 since the service is part of IBMS services.

UNISTAD WO ref. number: WO-03 (WK.DG1) – 20181022

		Title	Signature	Date
Prepared by	Muhammad Abdullah Rana I have prepared this document having identified SC requirements.	Ooredoo Project Manager		24.12.2020
Consult and supported by	Shantanu Deshpande I have reviewed and recommended this document for its accuracy and technical content, and to meet SC requirements.	Supreme Committee, Lead Business Analyst		04.01.2021
Reviewed and Recommended by	Suraj Seshadri I have reviewed and approved this document for its accuracy and technical content, and to meet SC requirements.	Supreme Committee, Tournament ICT Consultant		04 Jan 2021

Reviewed and Approved by	Mohammed Al Sayed I have reviewed and approved this document for its accuracy and technical content, and to meet SC requirements. *For Green Stadium Service Only*	Aspire Zone Foundation, Head of HVAC, Sports Facility Management		21-01-2021
Reviewed and Approved by	Hani Abdelaal I have reviewed and approved this document for its accuracy and technical content, and to meet SC requirements. *For Green Stadium Service Only*	Aspire Zone Foundation, Head of Mechanical Engineering, Sports Facility Management	 for green stadium services only	21-01-2021
Reviewed and Approved by	Hugh McCallum I have reviewed and approved this document for its accuracy and technical content, and to meet SC requirements.	Supreme Committee, FM Consultant		24 Jan 2021

Glossary & Acronyms

Name/Position	Description
ASF	Advanced Systems Format
COTS	Commercially Off The Shelf
CPU	Central Processing Unit
EBI	Enterprise Building Integrator
IBMS	Integrated Building Management System
I/O	Input Output
LAN	Local Area Network
MOI	Ministry Of Interior
OS	Operating System
UTP	Unshielded Twisted Pair
WAN	Wide Area Network
PSIM	Physical Security Information Management
SCTC	Supreme Committee appointed technical contractor
BMS	Building Management System

Contents

1. Introduction

Integrated Building Management Services, from this point forward referred to as the System or IBMS, is critical to the facility management and operation of the stadium and surrounding premises various building services.

1.1 Background UNISTAD Hub

The UNISTAD platform consists of a centralized infrastructure named Hub as depicted in the diagram below, local venue ICT infrastructure and all the connectivity between them and the external entities such as the National command centre, Broadcast centre, etc.

The Hub is setup on a cloud-based infrastructure which consists of a primary and redundant site where the common services would be hosted as depicted in the image below. Venues are stadiums, facilities and temporary sites such as fan zones which connect to the Hub and consume the various common shared services.

The venue would host basic infrastructure in a cloud to host a minimal set of services that are required for the independent operation of that venue.

This approach will ensure a consistent ICT technology footprint across the country for any major event making it easier to manage and maintain the ICT backbone, streamlines vendor management operations, reduces integration complexity, by benefiting from operational efficiency where ICT efforts will focus within a single technology hub and allows the country to provide a consistent set of services with the same quality levels to our visitors, stadium operators, FIFA and the LOC since the same set of services are being provisioned from the same central location.

1.2 Purpose

The purpose of this Business Requirements Specification is to identify Facility Management requirements for the System required following handover by the stadium contractor, in order to inform design development and delivery by the UNISTAD/SCTC solution provider.

This document will be used as the basis for the development of high-level design, technical specifications, testing and commissioning plans, training plans and handover documentation.

1.3 Scope

The requirements contained herein represent the current minimum required at Al Janoub Stadium.

The System shall provide an open system architecture that consolidates integration of various building services provided by Building Contractor into an integration layer. The System shall be integrated with following services but not limited to:

- UNISTAD Service ID 1.2 -Building Management Services
- UNISTAD Service ID 1.3 -Energy Management Services
- UNISTAD Service ID 1.5 - Water Management Service
- UNISTAD Service ID 1.6 - Indoor Lighting Control Services
- UNISTAD Service ID 1.7 - Flood Lighting Control Services
- UNISTAD Service ID 1.8 - Facade and Outdoor Lighting Services
- UNISTAD Service ID 1.13 – Green Stadium Services
- UNISTAD Service ID 2.3 - Integrated Venue Safety and Security Monitoring & Incident Management Services
- UNISTAD Service ID 2.8 - Intelligent Fire Management Service –

Requirement Stakeholders are represented by the column head “Stakeholder” in the requirements tables as:

- FM for SC - Facility Management
- TDO for SC - TDO Security
- SECC for Security Committee

The document does not include any tournament-specific requirements.

1.4 Requirements

1.4.1 Functional Requirements

The requirements will be captured based on UNISTAD standard templates that are provided as part of the project. The template referred to are part of the Design Phase for this project mentioned in the Reference section 2.

1.4.1.1 General

No	Description	Stakeholder
FN 1. General - Functional Requirements		
FN 1.1	The System provides the capability for centralized real time Monitoring & Control of BMS system and monitoring alarms from all integrated subsystems.	FM
FN 1.2	The System provides the capability for centralized real time Event & History Archiving	FM
FN 1.3	The System provides the capability for centralized real time Monitoring of Faults & Alarms	FM
FN 1.4	The System provides the capability for centralized real time collection of Energy data	FM
FN 1.7	The System provides the capability for Global Scheduling/ Time programs for all integrated subsystems.	FM
FN 1.9	The System is Centrally time synchronized using NTP protocol	FM
FN 1.11	Time Synchronization will allow for common time stamp for scheduling, history, events, alarms, archives etc.	FM

1.4.1.2 IBMS Operator Station

No	Description	Stakeholder
FN 2. IBMS Operator Station - Functional Requirements		
FN 2.2	An operator shall use IBMS Operator Station to perform a range of facility management tasks such as but not limited to: View, monitor alarms from all integrated subsystems.	FM
FN 2.3	An operator shall use IBMS Operator Station to perform a range of facility management tasks such as but not limited to: analyze the trend data acquired from various subsystems	FM

1.4.1.3 User Interface Requirements

No	Description	Stakeholder
FN 3. User Interface Requirements - Functional Requirements		
FN 3.12	The user interface shall implement a comprehensive log in and out username and password control system.	FM
FN 3.14	The system shall require all users to log on and shall record all actions of the user while logged on.	FM

No	Description	Stakeholder
FN 3.15	All interfaces shall require imposed complex passwords and shall include automated aging and minimal differs values. The system shall provide a hierarchical password model where users are to be given access to functions on the basis of Lvl1 (view only), Lvl2 (view & acknowledge), Operator (view, acknowledge & control), Supervisor (some configurations), Engineer (most of the configurations) and Manger (full access).	FM
FN 3.16	All software (applications, services, drivers and other software) required for a product, device or system to work shall automatically start without user intervention and shall not require a user to be logged in to the hosting computer or to actively start the application.	FM
FN 3.17	All software shall be designed to work with the operating system selected by the software author without fault or interruption, shall be wholly compatible with the selected operating system and shall include full error trapping and handling routines such that any faults or errors that may occur do not present to an operator or present a message that is in an understandable and meaningful format to an operator.	FM
FN 3.18	The system shall include automated log off. according to the requirement.	FM
FN 3.19	The user shall automatically be logged out following a period of system inactivity.	FM
FN 3.20	The period of inactivity shall also be configurable	FM

1.4.1.4 Alarm or Event Handling Requirements

No	Description	Stakeholder
FN 4. Alarm or Event Handling Requirements - Functional Requirements		
FN 4.1	All system and subsystem activity including alarm and every change of state of the system shall be logged as event or alarm based on the priority/severity.	FM
FN 4.2	Events are lower priority activities that require the user/operators to analyse the events and determine if further action is required.	FM
FN 4.3	Alarms are a higher priority event indicating a serious event that needs prompt operator action. All alarms shall require alarm acknowledgement (the operator shall acknowledge receipt of the alarm) and clearing (the alarms will be cleared automatically once actions are completed).	FM
FN 4.4	All and each action executed against an eventshall be recorded in the database to include the following: Field generated alarms & events	FM
FN 4.5	All and each action executed against an event shall be recorded in the database to include the following: The action (all user activity, to include details of any record changes, including the pre change value)	FM

No	Description	Stakeholder
FN 4.6	All and each action executed against an event shall be recorded in the database to include the following: The action originator (the user name)	FM
FN 4.7	All and each action executed against an event shall be recorded in the database to include the following: The date and time of the action to millisecond time precision	FM
FN 4.8	The event stack shall display events in text format scrolling up and down the computer screen displayed as a list.	FM
FN 4.9	The event list shall show all events from within the system and from all connected subsystems according to the default filtering applied according to the user log in or workstation configuration.	FM
FN 4.10	All alarms shall be assigned a priority (Urgent, High and Low).	FM
FN 4.11	Alarms with higher priorities shall require enforced operator handling.	FM
FN 4.12	Priorities shall dictate the order in which alarms to be actioned.	FM
FN 4.13	Events shall be displayed, sorted by date and time of event.	FM
FN 4.14	For alarms that require user/operator evaluation and potential further action the system shall allocate the alarms to the user/operator assigned to that area/facility. Once an alarm has been acknowledged the system shall not permit any form of de-acknowledgement or assignment to null.	FM
FN 4.15	The system shall provide an alarm stack, taking the form of a list of alarms presented for the operator to review or action.	FM
FN 4.16	The system shall support a process of alarm handling based on a process involving: Alarm acknowledge (accept by operator) => execute associated actions (manual action in the field) => close alarm (automatic closure of alarm in the system).	FM
FN 4.17	The system shall support "time to acknowledge" definable periods and the alarm shall be acknowledged within a defined period starting from the time (second) the alarm is received by the system. (FM team to decide the required functionality during operation)	FM
FN 4.18	Failure to acknowledge within the time window shall escalate the alarm priority and shall be recorded in the system's event record. (FM team to decide the required functionality during operation)	FM
FN 4.19	The reporting system shall allow reports on details of failures.	FM

1.4.1.5 Building Management Services

No	Description	Stakeholder
FN 5. Building Management Services - Functional Requirements		

No	Description	Stakeholder
FN 5.1	The System shall integrate with UNISTAD service ID 1.2 Building Management Services by collecting all the BMS related monitor and control integration points to be used in future advance Hub releases.	FM
FN 5.2	The System shall collect the respective BMS points which will enable future advance Hub releases in providing centralized BMS capabilities such as monitoring and control of various building equipment for analytical purposes, decision making and response.	FM

1.4.1.6 Energy, Water and Lighting Services

No	Description	Stakeholder
FN 6. Energy, Water and Lighting Services - Functional Requirements		
FN 6.1	The System shall integrate with UNISTAD service ID 1.3 Energy Management Services by collecting all the energy related monitoring integration points to be used in future advance Hub releases.	FM
FN 6.2	The System shall integrate with UNISTAD service ID 1.5 Water Management Services by collecting all the water related monitoring integration points to be used in future advance Hub releases.	FM
FN 6.3	The System shall integrate with UNISTAD service ID 1.6 Indoor Light Control Services by collecting all the indoor lighting related monitor and control integration points to be used in future advance Hub releases.	FM
FN 6.4	The System shall integrate with UNISTAD service ID 1.7 Flood Lighting Control by collecting all the flood lighting related monitor and control integration points to be used in future advance Hub releases.	FM
FN 6.5	The System shall integrate with UNISTAD service ID 1.8 Facade and Outdoor Lighting Services by collecting all the façade and outdoor lighting related monitor and control integration points to be used in future advance Hub releases.	FM
FN 6.6	The System shall collect the respective energy, water and lighting points which will enable future advance Hub releases for providing data to Command & Control system (by other) for achieving centralized capabilities for consumption overview, analytics, reporting and the identification of opportunities for consumption optimization. Note this is dependent on the downstream system to be configured to get such data.	FM
FN 6.7	The System shall collect the respective lighting points which will enable future advance Hub releases in providing centralized capabilities for zone specific comfort lighting control and smart scheduling of light. Note this is dependent on the downstream system to be configured to get such data.	FM

1.4.1.7 Integrated Venue Safety and Security Monitoring & Incident Management Services

No	Description	Stakeholder
FN 7. Integrated Venue Safety and Security Monitoring & Incident Management Services - Functional Requirements		
FN 7.1	The System shall integrate with UNISTAD service ID 2.3 Integrated Venue Safety and Security Monitoring & Incident Management Services for all the Safety and Security related services.	FM, SECC, TDO
FN 7.2	As part of the Safety and Security Monitoring, the System shall provide seamless integration with UNISTAD service ID 2.2 Unified Identity Management and Building Access Control Services.	FM, SECC, TDO

1.4.1.8 Intelligent Fire Management Service

No	Description	Stakeholder
FN 8. Intelligent Fire Management Service - Functional Requirements		
FN 8.1	The System shall integrate with UNISTAD service ID 2.8 Intelligent Fire Management Service by collecting all the fire management related monitoring integration points to be used in future advance Hub releases.	FM
FN 8.2	The System will monitor the fire zones as part of the life safety systems.	FM
FN 8.3	Centralized real time monitoring of necessary extinguishing & smoke extraction system	FM
FN 8.4	Identify & display the fire zone location of Fire Alarm and providing visual notification to the operators.	FM

1.4.1.9 Green Stadium Requirements

No	Description	Stakeholder
FN 9. Green Stadium Service - Functional Requirements		
FN 9.1	The system needs to provide the centralized real time access to Water, Energy and HVAC consumption data	FM
FN 9.2	The system needs to provide the steady state consumption data during non-event period	FM
FN 9.3	The system needs to provide the steady state consumption data during event period	FM
FN 9.4	The system needs to display the alarm based on the priority/severity for Water Energy and HVAC	FM
FN 9.5	The system needs to provide friendly user interface and easy to extract wherever possible	FM

No	Description	Stakeholder
FN 9.6	Alarm Monitoring - Compare the main meter data (Water & Energy systems) with the sum of sub meters as applicable in order to determine any leakage in between in the network and raise an alarm accordingly	FM
FN 9.7	Alarm Monitoring - Interlink the consumption (Water & Energy systems) with the related system such as if we have irrigation water consumption while the irrigation pumps are off or the irrigation controllers are off and raise an alarm accordingly	FM

1.4.1.10 User Accessibility Requirements

General

No	Description	Stakeholder
UAR 1. General - User Accessibility Requirements - Functional Requirements		
UAR 1.1	Reporting subsystem shall provide a simple and flexible way to extract information from the server database.	FM
UAR 1.2	The preformatted reports shall be available as a part of IBMS platform that shall be configured via IBMS workstation displays.	FM
UAR 1.3	System shall allow graphical interface for reporting system event, point history and real time point information.	FM
UAR 1.4	Users of Integrated Building Management System platform shall benefit from a single login with a fully integrated security context.	FM
UAR 1.5	Operators shall perform system configuration, system monitoring & control, alarm management, from a single IBMS workstation, promoting increased operational efficiency, removing operational silos and reducing training costs.	FM
UAR 1.6	IBMS System user interface features shall be like Microsoft windows software and run on standard Microsoft windows computers. Depending on the requirements, the operator/user shall be able to access integrated IBMS workstation.	FM
UAR 1.7	IBMS System clients shall provide a graphical user interface to use for interactions with the system. The operator interface shall display high-resolution colour graphics that can be tailored to the requirements of each individual facility. Extensive use of Web-style menus, toolbars, and icons shall allow intuitive navigation and fast access to important information. The operator interface shall be designed to accommodate novice and experienced operators alike.	FM

Reports

No	Description	Stakeholder
UAR 2. Reports - User Accessibility Requirements - Functional Requirements		

No	Description	Stakeholder
UAR 2.1	The following are sample reports that are available and additional reports can be defined by SC: RPT1 Alarm/Event: This sample reports lists a summary of alarms and events by location and by date and time.	FM
UAR 2.2	The following are sample reports that are available and additional reports can be defined by SC: RPT2 History Trend: The History Trend produces historical data for points that match the search criteria, and that have been configured for history collection. Historical data can also be shown in graphical form and you can also include event information for each point.	FM

Business Intelligence

No	Description	Stakeholder
UAR 3. Business Intelligence - User Accessibility Requirements - Functional Requirements		
UAR 3.1	For the technical support teams :Critical Faults status reports which provide real time information across venues	FM
UAR 3.2	For the technical support teams: History Charts and Points & Alarm Reports for all integrated subsystems.	FM
UAR 3.3	For Venue Operator: Real-time view of energy meter and facility operation data	FM
UAR 3.4		FM
UAR 3.5		FM
UAR 3.6	For Venue Operator: Single window operation of IBMS including Fire & Access control	FM
UAR 3.7		FM
UAR 3.8		FM
UAR 3.9		FM

1.4.2 Non-Functional Requirements

1.4.2.1 Performance & Capacity Requirements

Resilience

No	Description	Stakeholder
PCR 1. Resilience - Performance & Capacity Requirements – Non-Functional Requirements		
PCR 1.1	For achieving superior fault tolerance, the System shall be configured for high-availability architecture applications to operate in a redundant hot standby configuration.	FM
PCR 1.2	To achieve this level of reliability, the EBI server shall be available with two servers: one is dedicated as the primary server and the other acts as hot standby server.	FM
PCR 1.3	If the primary server encounters a problem, the standby server automatically assumes control and reconnects controllers and clients	FM
PCR 1.4	The redundancy solution shall insulate system against design faults, as servers shall not replicate all operating system software between the two servers, lowering the risk that malware or driver and Operating System problems could be not replicated to backup system.	FM

Scalability

No	Description	Stakeholder
PCR 2. Scalability - Performance & Capacity Requirements – Non-Functional Requirements		
PCR 2.1	System support up to 10,000 points for integration per stadium	FM
PCR 2.2	System supports up to 250,000 cardholders with unlimited access levels	FM

General

No	Description	Stakeholder
PCR 3. General - Performance & Capacity Requirements – Non-Functional Requirements		
PCR 3.1	Software Licenses and upgrades will be covered until Jan 2023	FM

Diagnostic and Error Handling

No	Description	Stakeholder
PCR 5. Diagnostic and Error Handling - Performance & Capacity Requirements – Non-Functional Requirements		

No	Description	Stakeholder
PCR 5.1	IBMS system shall include a powerful Diagnostic Framework application that shall provide a unified interface for running tests, recording system activity, collecting diagnostic information, and viewing logs.	FM
PCR 5.2	It shall contain a set of pre-defined tests that are applicable to the system and the current operating environment.	FM
PCR 5.3	The tests shall vary depending on whether the Diagnostic Framework is installed on a server or a client computer.	FM
PCR 5.4	The tests shall be comprehensive and typically shall be consist of a number of sub-tests. For example, a system health test includes sub-tests for versions of OS components, status of services, security configuration, and so on.	FM
PCR 5.5	The Diagnostic Framework shall contain a set of pre-defined recording profiles that define what system activity and parameters to record for particular types of problems.	FM

1.4.2.2 Reliability Requirements

Backup, Restore & Archiving

No	Description	Stakeholder
RR 1. Backup, Restore & Archiving - Reliability Requirements – Non-Functional Requirements		
RR 1.1	The System shall allow performing backup of important data such as the server database for avoiding loss of data in the event of hardware or software failure (such as a hard disk crash) occurs, files are accidentally deleted or in the event of a natural disaster, such as a flood or fire.	FM
RR 1.2	Choosing an appropriate backup strategy shall be in place for minimizing the downtime due to various situations that cause loss of data.	FM
RR 1.3	Appropriate backup strategy shall be chosen considering the types of situations that can occur: Media failure—if one or more disk drives fails, there is a potential for a complete loss of data unless the system was properly backed up.	FM
RR 1.4	Appropriate backup strategy shall be chosen considering the types of situations that can occur: User error—if a user makes invalid modifications to data, for example, modifying detection settings, an effective way to undo these changes is to restore the data from backup.	FM
RR 1.5	Appropriate backup strategy shall be chosen considering the types of situations that can occur: Permanent loss of a server—if a server becomes permanently unusable, for example, due to natural disaster.	FM
RR 1.6	Backups being a CPU and disk intensive operation on a large system. It shall be best to be performed backups at quiet times.	FM

RR 1.7	It shall ensure that no data is lost if the Server database is corrupted or destroyed, it is important that the database is backed up regularly.	FM
RR 1.8	Some of the SQL Server databases have a daily backup job configured automatically when installed. The database backup shall be copied from the IBMS server to another location in case of hard disk failure.	FM
RR 1.9	A general backup strategy is: Full backups run weekly.	FM
RR 1.10	A general backup strategy is: Incremental backups run daily.	FM
RR 1.11	A general backup strategy is: Manual backups as needed.	FM
RR 1.12	As part of Disaster Recovery strategy, a comprehensive backup and restore policy for disaster recovery purpose shall be defined.	FM
RR 1.13	A disaster recovery plan shall form part of an overall business continuity plan or strategy that identifies the critical business systems and resources that support those systems.	FM
RR 1.14	A risk analysis of those business systems shall be performed to determine a disaster recovery policy or plan.	FM
RR 1.15	In formulating this policy following shall be considered: • How quickly data or the system needs to be restored. This will indicate the need for a redundant system, spare offline computer, or simply good file system backup. • How long data needs to be kept. • The frequency of changes to critical data and configuration settings. This will dictate the frequency and completeness of backups. • The safe onsite and offsite storage of full and incremental backups. • The safe storage of all Microsoft operating system and IBMS related installation media, license keys, and configuration information. • Whether offsite recovery and analysis is required. Some sites require offsite recovery and analysis to determine the cause of the incident.	FM

1.4.2.3 Security & Privacy Requirements

User Access

No	Description	Stakeholder
SPR 1. User Access - Security & Privacy Requirements – Non-Functional Requirements		
SPR 1.1	Following is a sample list of stakeholders or users who will use the system. Additional users can be added as required by SC and roles can be defined:	FM

	Operator: Capacity to view and control the system. The user should possess system operation knowledge.	
SPR 1.2	Supervisor: Capacity to view, control, analyse and report on the system. The user should possess system operation knowledge.	FM
SPR 1.3	Maintenance Technician: Capacity to view, control and maintain the system. The user should possess system operation & basic configuration knowledge	FM
SPR 1.4	Engineer: Capacity to configuration of the system. The user should possess details system configuration knowledge	FM
SPR 1.5	Manager: Super User, ability to have full configuration and administration of the system. The user should possess detailed system configuration and administration knowledge.	FM
SPR 1.6	The System shall support the complex requirements of large geographically distributed systems.	FM
SPR 1.7		FM
SPR 1.8		FM
SPR 1.9		FM
SPR 1.10		FM
SPR 1.11	IBMS System Network shall secure access to the operating system by ensuring that: Only authorized users have access to the system.	FM
SPR 1.12	IBMS System Network shall secure access to the operating system by ensuring that: User access to files, systems, and services is limited to those necessary for the performance of their duties.	FM

1.4.2.4 User, System & Support Documentation Requirements

Training & Handover

No	Description	Stakeholder
DOC 1. Training & Handover - User, System & Support Documentation Requirements – Non-Functional Requirements		
DOC 1.1	Training tailored to the Al Janoub implementation, shall be provided to the user groups listed in 1.3.2.3 in addition to Security stakeholders and Client representatives.	FM
DOC 1.2	Training shall be user group / role-specific and include the following delivered in English: Manuals	FM
DOC 1.3	Training shall be user group / role-specific and include the following delivered in English: Presentation	FM
DOC 1.4	Training shall be user group / role-specific and include the following delivered in English: Live system demonstrations	FM
DOC 1.5	The entire training documentation such as presentation material and User account shall be tailored to the Al Janoub	FM

	implementation and shall be submitted for review and approval prior to the training programme.	

1.4.2.5 Testing Requirements

Testing & Commissioning

No	Description	Stakeholder
DOC 1. Testing & Commissioning - 1.3.2.5 Testing Requirements – Non-Functional Requirements		
TR 1.1	Integration testing with Building BMS System is necessary for ensuring that supplied BMS System points can communicate with IBMS System.	FM
TR 1.2	IBMS operator workstations Integration Testing.	FM
TR 1.3	Stress/Load Testing: Stress/Load testing to be performed to ensure that the system operates effectively without loss of performance in realistic, high network traffic conditions.	FM

2. References

Following is the list of references.

Reference "UNISTAD_IBMS_Interface_IO_Class_information_gathering_for_Al-Janoub_Stadium_Revx.x" for Integrated Building Management system design input details.

3. Modification to requirements.

The requirements for video Surveillance and CCTV have been removed/modified from the IBMS scope since they will be covered in UNISTAD HUB and not in the IBMS.

- Requirement modified by removing CCTV references – FN 1.11, FN 2.1, FN 3.3, FN 3.6, UAR 1.5, UAR 3.4, UAR 3.5, UAR 3.6, UAR 3.10
-
- Requirement modified by removing ACS references – FN 1.1, FN 4.4 to FN 4.7, FN 4.16 to FN 4.18, FN 4.19, FN 6.6, FN 7.2, UAR 1.3, UAR 1.5, UAR 2.1, UAR 2.2.

- Requirements removed since they were for CCTV -
    - FN 1. General - Functional Requirements :
      The System provides the capability for camera configuration, viewing & management
    - FN 3. User Interface Requirements - Functional Requirements
      The mapping system shall include dynamic CCTV image presentation within/over the map. CCTV associated with alarms shall be presented in the CCTV window.
    - FN 7. Integrated Venue Safety and Security Monitoring & Incident Management Services - Functional Requirements :
      As part of the Safety and Security Monitoring, the System shall provide seamless integration with UNISTAD service ID 2.1 Video Surveillance and Security Analytics Service which will enable various features not limited to viewing camera playback and controlling PTZ cameras.
    - UAR 3. Business Intelligence - User Accessibility Requirements - Functional Requirements
      For Security Team: View cameras, playback recordings, forensic analysis on recorded video, export selected video for evidence.

- Requirements removed since they are not applicable
    - User Acceptance Testing: User Acceptance Testing of system to demonstrate full functionality and performance in accordance with specified requirements and agreed use-cases.
    - Integrated User Acceptance Testing: This will demonstrate full functionality of integration between the system and other systems and services.
- Requirement removed since they were for ACS –
-
    - FN 1.5 The System provides the capability for configuration of doors & access rights for card holders
    - FN 1.6 The System provides the capability for integrating with an external card management system.
    - FN 1.8 The System provides the capability for Operator HMI -Custom graphics for Access Control
    - FN 1.10The System provides the capability for seamless integration with the VMS for Graphic Maps, Alarm, event and reports for Access Control.

- FN 2.1 The System Operator Station shall provide a high resolution, color graphical Human Machine Interface (HMI) software to the Server for centralized real time monitoring & control of Access Control.
- FN 3.1 The user/operator shall be assigned a screen display layout of areas/facilities and will have access to those areas/facilities, which are appropriate to their job functions.
- FN 3.2 The System shall support and provide a mapping /display solution.
- FN 3.3 The mapping system shall include dynamic and animated icons that shall change state in real time according to the status of the object, which they represent with regards to Access Control.
- FN 3.4 The System icons shall be large enough to allow a user to easily select them.
- FN 3.5 To avoid clustering icons in heavily populated map areas the maps shall be so arranged and layered to ensure that icons do not overlay one another, that selection of one icon amongst a group or cluster of icons is easy and can be executed without inadvertently selecting the wrong icon.
- FN 3.6 Icons shall include context sensitive right click menus to provide details of status or options, variables or properties of the object being represented for Access Control and.
- FN 3.7 The system shall provide dynamic drill down on receipt of an alarm or event.
- FN 3.8 Mapping configuration shall, however, allow workstations to be dedicated to specific areas of the building or site and in this arrangement only those maps for the area associated with the workstation shall be available to the operator logged in at the workstation.
- FN 3.9 All maps have navigation controls and shall include: Return to the home page
- FN 3.10All maps have navigation controls and shall include: Move up and down one layer;
- FN 3.11All maps have navigation controls and shall include: Move side to side on the same layer (where the site is depicted in tiles)
- FN 3.13The user interface shall host a database of users/operators with associated rights to make visible and grant or deny differing levels of access to each system function.
- UAR 3.4 For Venue Operator: Find a point in alarm and navigate to relevant graphics pages to investigate issues related Access Control
- UAR 3.5 For Venue Operator: Simple point & click operation on for Access Control Services
- UAR 3.7 For Security Team: Manages access rights configuration & assignment
- UAR 3.8 For Security Team: Supervision and management of cardholder data, expiry date etc.
- UAR 3.9 For Security Team: locking & unlocking gates from security HMI
- SPR 1.7Using the Enterprise Model, each site/facility shall be logically partitioned into separate locations and cardholders are logically partitioned into separate organizations.
- SPR 1.8Each location / organization shall have a logical set of points, cardholders, cards, reports, and displays.
- SPR 1.9Each operator shall then be allowed to view, monitor, and control only those points or cardholders within their designated location or organization.
- SPR 1.10 In this way, operators shall be prevented operators from viewing information from another part of the system that is not relevant to them.