
Associated Total Offender Management System [ATOMS]

TABLE OF CONTENTS

Introduction.....	3
Objectives And Overview	4
Technical Terms And Conditions	5
System Development And Implementation Approach.....	5
Requirement Analysis.....	5
System Architecture	5
System Security	6
Platform And Technology.....	6
Infrastructure And Network	6
Warranty Support And Maintainance	7
Backup And Recovery	7
Training And End-User Development.....	7
Ownership Of Source Code And Other Property	7
General Terms And Conditions.....	9
Evaluation Criteria And Methodology.....	9
Annexure I	10
Scope Of Work.....	10
Annexure II.....	12
System Requirement Overview	12
1. Detainee Profile.....	12
2. Pshycological history management.....	13
3. Case Management	13
4. Remand Order/Sentence Execution Management.....	13
5. Medical Management.....	14
6. Prison Sentence Execution Management	15
7. Parole, Clemency and other pardon management	17
8. House Arrest And Island Banishment Execution.....	18
9. Community Service Execution	18
10. Rehabilitation Framework Management.....	19
11. Correctional Facility Management	20
12. Document Management.....	21
13. Human Resource Management.....	21
14. Intelligence Management.....	22

15. Correctional Institute Management.....	22
Annexure III	24
Change Request Contract (CRC)	24
Annexure IV	25
Non-Disclosure Agreement	25

[REMAINDER OF THIS PAGE LEFT BLANK INTENTIONALLY]

INTRODUCTION

Formed on the 31st of December 2013 under the Prisons and Parole Act 14/2013, the Maldives Correctional Service (hereafter referred to as MCS) is responsible for the responsibilities mandated to MCS by law.

1. Operate the Maldivian prison system according to reliable procedures,
2. Build a safe and secure prison environment for offenders,
3. Provide training to offenders to teach them various skills,
4. Help offenders to reform and encourage them to return to society as a worthy citizen after being released from custody,
5. Compile procedures to serve sentences as per the court ruling, and
6. Compile procedures and arrange detention centers for offenders or persons remanded to appear in a court in the future or held in custody for the duration of an investigation of an institution with authority.

MCS works with local and international bodies to ensure adequate operations and complete adherence to the laws, rules, and regulations of the Government of Maldives (hereafter referred to as GOM) and international protocols, conventions, and other pacts GOM is a party to.

At present, MCS employs nearly 700 staff responsible for more than 2,000 inmates and detainees of different categories in its facilities, while more than 200 are under surveillance in Male', Maldives' capital.

Since the required documentation, logs, and other vital information of these services aren't systematically recorded or logged, data is either not available when needed or inconsistent and unreliable.

[REMAINDER OF THIS PAGE LEFT BLANK INTENTIONALLY]

OBJECTIVES AND OVERVIEW

This project aims to provide MCS with a modern-day comprehensive software solution for its management, which would speed up the processes; improve its efficiency by appropriating MCS employees in daily operations rather than employing them to process information.

With this solution's establishment, MCS is to gain the community's trust of the governing and monitoring bodies. The solution should be dynamic, easily adaptive to changes, and scalable based on MCS workflows and operational procedures with perfect adherence to the laws, rules, and regulations of the Republic of Maldives and the international pacts and other related conventions. Data stored and manipulated via the software, expected to be secure, highly available, robust, and resilient.

The system should introduce automation into MCS management to improve security, facilitate better monitoring and care for inmates and those in remand, improve efficiency and provide in-time visibility of the prison system's state for better management decision making.

The system should have measures to catalog actions by employees, inmates, and those under remand, including conversations between MCS inmates and employees, other stakeholders, and responses.

The system should integrate with the processes and related hardware to update seamlessly as part of the live workflow, logging and manipulating data in real-time.

[REMAINDER OF THIS PAGE LEFT BLANK INTENTIONALLY]

TECHNICAL TERMS AND CONDITIONS

SYSTEM DEVELOPMENT AND IMPLEMENTATION APPROACH

The system should be modular (See System Architecture for more details). The vendor should clearly define the number of modules or functions that they believe would be core to their proposed systems and the modules deployed in a phased approach.

The development lifecycle, acceptance testing procedures, and deployment should be proposed and agreed upon by MCS before the commencement of work or during the steering process.

Procedures for error-corrections and updates during UAT phases and post-production should be defined and agreed upon by both the developer and MCS.

REQUIREMENT ANALYSIS

The vendor has to conduct a thorough analysis of the existing systems and functions at MCS to arrive at an optimal solution that would work seamlessly integrated with MCS's current hardware, operations', process, and flow. The analysis involves the assessment of processes in related agencies if required.

Aside from the case study conducted, it is expected from the vendor to grasp a fair understanding of the protocols, conventions, and other international laws, rules, and regulations that GOM follows to ensure that the system's workflows comply with the required standards. Annexure of this document contains a list of some documents that provide details about these standards.

In their system study document, the vendor is welcome to recommend changes to processes and workflows to enhance the system's integrity, availability, security, and adherence to protocols and conventions that MCS is a party to.

Once the study is complete, the proposed system document is subject to approval by the Steering Committee of the project, a committee formulated by bringing together key personnel from relevant authorities.

Bidders/ Vendors are required to submit the decisive copy of the user requirements and system specifications with no copyright or legal limitations.

Annexure II of this document contains a brief overview of the workflow and high-level user requirements that further describes the project's work scope.

SYSTEM ARCHITECTURE

The system should be designed and implemented in a modular fashion. The modules should have APIs or services in place for seamless integration with other modules. The modular separation allows for ease of development, bug fixing, and phasing out of the entire solution.

The vendor would map out the modules in their proposed solution, with a clear distinction of core and additional modules with timelines for delivery. If vendors find additional modules that were

not identified as part of the case study but might improve the system's availability, efficiency, performance, or security, vendors are welcome to include details for further evaluation.

SYSTEM SECURITY

All users of the system, including the entities that utilize any services, APIs or web portals, or any services mentioned earlier, are expected to authenticate before using the system.

The system should support an industry-standard multi-factor authentication.

Data encryption, masking, and other forms of data security should be inherent to the system design.

Thorough and comprehensive logging of every transaction that happens through the system should be an integral feature of the system. All actions should have an audit journal that is utilizable for accounting purposes. Manipulation or deletion of these audit logs should only be allowed for system administrators. The solution's proposal should document the depth of logging and measures to ensure these audit trails' integrity.

The system's operations must have a level(s) of authorization with roles defining every function. Each role should consist of permission(s) that reflect the permission of each action.

Authorization and access to encrypted data only via digitally verifiable systems should be a key feature in the system.

The vendor should adopt and recommend industry-standards and best practices to assure system and data integrity. Vendors should specify in detail industry standards and best practices they would use to deter and minimize exploiters from tampering, altering, or deleting the data stored due to any design flaw(s), bug(s), or any misconfiguration(s) of the system.

PLATFORM AND TECHNOLOGY

The vendor should specify the platforms, technologies, and libraries they adopt to build the solution, clearly defining the adoption reasons. Vendors should detail any proprietary technology they would be utilizing, including fees for licensing incurred, if any.

INFRASTRUCTURE AND NETWORK

MCS shall instruct the vendor on the details of the deployment as required. A distributed network would securely connect the primary data center that hosts the application with remote locations where it is accessed.

The system must be highly available to function offline at distributed facilities at times of network disconnections or unreliable network conditions. The vendor may recommend the preferred network requirement(s) for such a distributed deployment.

[REMAINDER OF THIS PAGE LEFT BLANK INTENTIONALLY]

WARRANTY SUPPORT AND MAINTAINANCE

Providing free bug fixes, patches, and other maintenance tasks for the system, from a component going into production to complete acceptance testing of the product, is a vendor's responsibility. The proposal should specify the rate and details of an annual maintenance commitment, including support levels and maximum inflation rates of renewal, if any, for subsequent years.

Optionally, the vendor may propose additional maintenance and support contracts to extend the implemented system's maintenance and support. The agreement should facilitate bug fixes and other maintenance-related operations accordingly. Once the contract expires, the vendor may provide necessary development, enhancements as required on a payment basis.

Onsite support is mandatory and should be provided within a maximum of 3 hours in case of a system failure or discovering a critical bug.

As previously mentioned, MCS personnel should test all bug fixes, patches, updates, upgrades, or any amendment(s) before rolling out into production. Bugs, flaws, and vulnerabilities discovered in this testing phase should be classified and treated as mentioned in the System Development And Implementation Approach.

BACKUP AND RECOVERY

The system should have a functional backup regime. Backup and Disaster Recovery tools would be the responsibility of the infrastructure solution and are outside the scope of the vendor.

TRAINING AND END-USER DEVELOPMENT

The vendor should train all users that require access to the system, including users from other stakeholder agencies.

A web-based form of User Technical Documentation and System Design Documentation is compulsory. The system should have a training/staging environment where users may experience and use the staging/training environment.

The training environment should be a replica of the production system. All updates, patches, and bug fixes should be reflected in the training environment as they happen, even if brought after the system implementation.

All technical administrators of the system should undergo required training to maintain the system, including getting certified to support proprietary technologies used in the system. The vendor should provide all costs and training formalities.

OWNERSHIP OF SOURCE CODE AND OTHER PROPERTY

Version control of source code, configurations, and other related property, with changelogs, are to be systematically maintained.

Once the system's implementation is complete, the vendor should hand over all intellectual property such as source code and configurations to MCS with full ownership.

Hardware provided as part of the system should be correctly listed and be acknowledged by MCS and the vendor as the property of MCS.

[REMAINDER OF THIS PAGE LEFT BLANK INTENTIONALLY]

GENERAL TERMS AND CONDITIONS

EVALUATION CRITERIA AND METHODOLOGY

- Maldivian software ventures, with relevant expertise and reputation of delivery of quality and timely project delivery would be given priority.
- An evaluation committee formalized by MCS, which consists of 5 members, would judge initial proposals from bidders to shortlist a maximum of 5 bidders in the following criteria
 1. The bidder's approach on the system according to the Work scope (Annexure) defined in this document.
 2. Documents that prove financial capability to support the project.
 3. Documents that provide a brief Human Resource plan of the bidder's team and its member's competency.
 4. Documents that provide details about previous experiences and testimonials from previous clients
 5. Project timeline, Terms Of Project Delivery And Implementation
- Shortlisted 5 bidders are requested to complete a system study within MCS and other stakeholders.
- Once the study is complete, the bidders should prepare the following
 1. A working mock of the proposed system
 2. Complete HR plan with resource manning details after a detailed scope identification
 3. A Presentation that proves their understanding of the undertaking's scope and depth by the completeness of the proposed solution.
- The parties should present the mentioned presentation and demonstration to an interview panel that consists of
 1. 1 Member of the evaluation committee from MCS
 2. 1 Member Appointed By The Government Of Maldives
 3. 1 Independent Industry Expert
- Parties that complete the presentation shall be requested to submit their best and final financial offer.
- Once the best and final financial offer submissions are complete, The contract shall be awarded to the bidder to demonstrate the best fit product according to the marking scheme below.

Criteria	Marks (%)
Competency as a team, including company details	10
Evaluation Committee Score	30
Interview Panel Score	20
Best And Final Financial Offer	35
Delivery Terms	5

ANNEXURE I

SCOPE OF WORK

- Get to know the operational procedures of MCS and prepare a case study on digitizing the workflow required to develop a modern-day, future proof software solution. This study should also include the best practices, recommendations, protocols, and international conventions related to human rights, prison management, inmate management, and correctional services we are party to; Mandatory documents are listed below:
 - European Prison Rules (<http://bit.ly/1HwP4Sa>)
 - The United Nations Standard Minimum Rules for the Treatment of Prisoners (the Nelson Mandela Rules) (<http://bit.ly/2GyXgVW>)
 - UN Standard Minimum Rules for the Treatment of Prisoners (<http://bit.ly/37BNrCK>)
 - UN Bangkok Rules (<https://bit.ly/2PWEvRA>)
 - UN Beijing Rules (<https://bit.ly/39yFWxp>)
 - UN Tokyo Rules (<https://bit.ly/3dog384>)
- The vendor must specify the documentation and design strategies and detail the software development methodologies and lifecycle they would adopt.
- Identify and streamline data migration required for the system. Once complete, the vendor should provide MCS with instructions for data migration required for the system and ensure data transfer completion before rolling out each module. The testing should consider the data migration aspect, and as such, the vendor must address issues that arise.
- Ensure that the software interface is developed in "Dhivehi" using a Thaana font approved by the GOM. However, Interfaces such as the medical module and some services and applications accessible and utilized by foreigners should be in a dual language manner.
- Develop a comprehensive, modular, secure, highly available, resilient Management System to automate detainee and prison management services of the Maldives Correctional Service. Principal components can be, but not limited to, as described in Annexure II of this document.
- The software should run through individual tests that confirm the software's validation and development, at least in the headquarters and the prison(s) with the highest population. Each location is to have an assigned tester at the time of implementation. Once the tests are complete with comprehensive supervision from the designated testing supervisor and dependent on the test results, the software is subject to be developed to the extent needed from the nominated tester(s) or supervising tester of MCS.

- The vendor is to provide the following once the implementation is complete
 - Source code
 - Software drivers and license keys where necessary
 - System files needed for installation and execution
 - Web-based User Manual which consists of:
 - Operational Manual
 - User Manual
 - Knowledgebase of known bugs
 - System Design
 - Technical Feature(s)

[REMAINDER OF THIS PAGE LEFT BLANK INTENTIONALLY]

ANNEXURE II

SYSTEM REQUIREMENT OVERVIEW

1. DETAINEE PROFILE

1.1. Bio Data

- 1.1.1.A person's traits inclusive of information about the person, including identity, nationality, and other relevant information.
- 1.1.2.History related with MCS executions and intelligence should also be linked accordingly.
- 1.1.3.Communicate with API's and services of government to fetch and provide most up to date data with related governmental institutes.

1.2. Medical Profile

- 1.2.1.A complete medical history inclusive of information related to chronic disease and other medical information that may be required globally in the system.
- 1.2.1.1. Example: No Cuffing, requires wheel chair and etc.

1.3. Physiological Profile

- 1.3.1.A complete psychological profile inclusive of special treatments and information about the profile that maybe required globally in the system.
- 1.3.1.1. Example: Suicidal Behavior, Bipolar Disorders etc.

1.4. Employment and Educational Information

- 1.4.1.All information provided by the prisoner or related authorities about education and employment.

1.5. Relation with Gangs and Terrorist Organizations

- 1.5.1.Map profile(s) of the person(s) related to gang(s), terrorist organization(s), and other group(s) of misconduct by utilizing information provided by intelligence information gathered by MCS or governmental authorities about the person.

1.6. Family History and Relations

- 1.6.1.Use methods of verification to verify the authenticity of the family information provided.
- 1.6.2.Manage history of spouses and children as available for visit purposes.

1.7. Imaging of Scars, Cuts, Bruises, and Other Birthmarks

- 1.7.1.Storage and management of temporary and permanent scars, cuts or bruises, and other birthmarks for medical, personal identification, and investigative purposes if required.

1.8. Biometrics

- 1.8.1.Mechanisms to record biometric data for profiles. Ability to port to an available ABIS system for identification and verification. The solution need not have a comprehensive ABIS system as part of the solution but may adopt biometric matching features for identification within the system.

1.9. Classification of Security Level

- 1.9.1.An automated algorithm assumes the person's security category and rates the person depending on the intelligence information of both prosecuted, unprosecuted crimes, suspicions on the person, and previous sentence executions.

1.10. Information and Action Requests

- 1.10.1. Requests for information about the person from relevant authorities are to be pushed via an API provided by the relevant authority

- 1.10.2. Request(s) for actions to be taken against the person to be pushed via an API provided by the relevant authority.
- 1.10.3. An API, Web service, Or an Application (portal) to handle requests from authorities.

2. PSYCHOLOGICAL HISTORY MANAGEMENT

2.1. Initial assessment

- 2.1.1. Initial assessment of person when brought to custody to be stored and history of these should be maintained.

2.2. Review Of Psychological profile

- 2.2.1. Review of profile with specific triggers such as recommendations from duty officers and self-requests should trigger an assessment
- 2.2.2. Comparison of reviews and history of psychological history.

2.3. Recommendation and prescription of programs and other counseling

- 2.3.1. Generate or let councilors prescribe programs and other counseling sessions to help remediate issues noticed in assessments.
- 2.3.2. Recommendations and history to be suggested when doing rehabilitation programs.

2.4. Collaboration with Medical

- 2.4.1. Though this module is independent, it should collaborate with the medical module to handle severe psychological cases.

3. CASE MANAGEMENT

3.1. Sentence(s) and appeal(s)

- 3.1.1. Management of sentence(s) and the verdict(s), remand orders, and other such orders from the judiciary.
- 3.1.2. An API, web service, or application allows courts to push agendas and other related information from the judiciary to identify the status, location, and additional information about the required person.
- 3.1.3. An API, web service, or application allows the judiciary to push notifications about hearings and other appearances required by the courts.

3.2. Investigative case(s)

- 3.2.1. An API, web service, or an application that allows related authorities to schedule appointments or generate "summon request(s)" for investigative purposes.

3.3. Previous Sentence and Execution Score Calculation(s)

- 3.3.1. An API, web service, or an application that allows the judiciary to look into the personnel's profile and summarize personal information and the criminal record for sentencing and other judgment references.

3.4. Document Management

- 3.4.1. Management of physical documents from different sources not in digital form is to be scanned, uploaded, sorted, and managed via the solution in an easy to fetch manner.

4. REMAND ORDER/SENTENCE EXECUTION MANAGEMENT

4.1. Change of Sentence/Remand Execution

- 4.1.1. Automatically change the sentence that under execution depending on the most recent sentence/remand order.

4.2. Auto Calculation of execution

4.2.1. Communicate with relevant modules to pause and resume sentence execution.

4.3. Transfer of prison and execution type for juveniles

4.3.1. Once juveniles reach the age determined by the law, regulations, rules, notifications should be raised so that the institution may transfer the juvenile to an adult correctional facility to resume the execution of the sentence.

5. MEDICAL MANAGEMENT

5.1. Medical Board Management

5.1.1. The management of medical board personnel and changes as they occur.

5.1.2. Scheduling of meetings.

5.1.3. Elevation of requests from doctors, family, and inmates on amendment or change of method for the sentence execution and subjected to a medical board decision.

5.2. Medical History Management

5.2.1. According to the person's information, family, medical documents, and previous medical conditions in the person's medical history, the system manages a person's medical history.

5.3. Medical Document Management

5.3.1. Management of previous and new medical documents that are not in digital form scanned by the user, uploaded, sorted, and managed via the system in an easy to fetch manner.

5.4. Acute and Chronic Medical Condition Management

5.4.1. Medical conditions that require permanent medication and special treatment marked on the profile to notify of needed special treatment

5.4.2. Medical conditions that may require special diets, allergies, and other food/utensil related issues indicated on the profile

5.5. Medication & Prescription Management

5.5.1. Information about ongoing medication, any medication information available via documents, family, or any related authorities

5.6. Family Medical History Management

5.6.1. Family history and suspicious symptoms to be stored to provide cautious handling

5.7. Sentence Execution Management

5.7.1. Alter the method of execution for the sentence concerning the decision of the medical board.

5.7.1.1. Example: If the medical board decides that the inmate may be allowed to go abroad for further treatment, the sentence execution should stop until the inmate returns after medical treatment.

5.8. Medical requests consultations and follow-ups

5.8.1. Requests for primary medical care, health care, and response management

5.8.2. Specialist referral and emergency medical situation management

5.8.3. History of consultations and follow-ups.

5.9. Investigations and results

5.9.1. History of requisitions, appointments for medical investigations.

5.9.2. Management of result collection and development of an API that pushes medical investigation results.

5.9.3. Connection to government proposed central medical database.

5.10. Pharmaceutical management

- 5.10.1. Management of pharmacies (modification and related equipment) stock.
- 5.10.2. Procurement and history of medical equipment.
- 5.10.3. Generation of restocking requests.
- 5.10.4. Generation of medication from external pharmacies.

5.11. Medical Center Management

- 5.11.1. Management of medical facilities managed by MCS.
- 5.11.2. Medical staff, doctors and nurses' management
- 5.11.3. Ward beds and equipment management
- 5.11.4. Consumables and other related accessory management. Related to pharmaceutical management.

6. PRISON SENTENCE EXECUTION MANAGEMENT

6.1. Initial Assessment management

- 6.1.1. Generate initial medical, psychological and other relevant assessments and feed assessment data into relevant functions such as
 - 6.1.1.1. Medical management
 - 6.1.1.2. Bio Data
 - 6.1.1.3. Psychosocial profile
 - 6.1.1.4. Security rating
 - 6.1.1.5. Parole and programs

6.2. Sentence Execution

- 6.2.1. Execute sentence based on prison type.
 - 6.2.1.1. Juvenile correctional facilities have different rules, regulations and execution terms. So the whole sentence execution instance should go by these mentioned rules, regulations and execution terms.

6.3. Prisoner Belonging Management

- 6.3.1. Management of all items confiscated at the time of prison entry.
- 6.3.2. Track the location of the belongings as it relocates.
- 6.3.3. Provide means of easy storage, tracking, and identification of confiscated items

6.4. Grievances, Complaints, and Notice Management

- 6.4.1. Management of grievances, complaints from offenders' or those under remand.
- 6.4.2. Required hand over document(s), notice(s), letter(s) management.

6.5. Prisoner Letter and Mail Management

- 6.5.1. Management of All Incoming and Outgoing Mail/ Letters from and to Inmates
- 6.5.2. Provide Tracking Information For Individual Mail/ Letters

6.6. Rights and Privilege management

- 6.6.1. Assignment and management of necessities such as pillow(s), toothbrush (es), and others as per law, rules, and regulations.
- 6.6.2. Assignment and tracking of phone calls as part of privilege.
- 6.6.3. Management of visits from the family, lawyer, and spouse per the law, rules, and regulations.
- 6.6.4. Management of requests for purchase from the Prison canteen.
- 6.6.5. Management of suspension(s) of specific privileges due to bad conduct.

6.7. Cell assignment

- 6.7.1. Automatically assign a cell to the person with an automated algorithm that determines the most appropriate cell dependent on rival gang(s), type of crime, and history.

6.8. Behavioral Assessment

6.8.1. Dynamic changes on a person's rating about the event(s) and actions(s) taken concerning the person.

6.9. Inter-prison Employment

6.9.1. Management of employment opportunities, attendance, and payroll management of inmates that work inside the prison.

6.10. Medical Center And Notification Management

6.10.1. Medical Complaints logged and lodged to medical centers accordingly

6.10.2. Maintain track and history of medical requests

6.10.3. Medication notification and medication chart generation

6.11. Educational, Vocational and Rehabilitation Activity Management

6.11.1. Enrolment of inmates in educational opportunities and other opportunities provided as rehabilitation activities.

6.11.2. Management of attendance, grading, and other institutional tasks

6.12. Security Rating

6.12.1. Dynamic, up-to-date ratings dependent on the types of crime(s) committed, the suspicion(s), action(s), and events in the system

6.13. Generation of Prison, Unit, Wing, and Cell Logs

6.13.1. Use of SDK's or API's of the hardware devices (if any) used to generate automated logs on the user and relative information about door open and close events.

6.13.2. In the absence of any hardware, as mentioned previously, all events of door opening are to be logged in minimum with the following details (Though this is the case, the system should be developed in a manner that hardware integration possible)

6.13.2.1.1. Location of the Key that the user used

6.13.2.1.2. Handover of key

6.13.2.1.3. The person who opened the door/gate

6.13.2.1.4. Timestamps

6.13.2.1.5. Authorization Information

6.14. Inter-Prison Transfers

6.14.1. Management of transfers between units, wings, and cells.

6.15. Escort Management

6.15.1. Management of the emergency support group that handles escorts in and outside the prison premises. In case the escort needs to be done on another island, automatic notification to MCS, Maldives Police Service, or an office on that island informing about the situation.

6.15.2. Bookings for MCS vessel(s), vehicle(s).

6.16. On-Demand Statistics

6.16.1. Prison statistics, such as alert levels and other relevant information.

6.16.2. Information includes head counts of inmates and officers in the prison area to be logged into the system after a physical count. The staff who conducted the headcount should sign off the previously mentioned information.

6.16.3. Integration with portable biometric devices to ensure the integrity of the headcount.

6.17. Notifications and Alerts

6.17.1. Senior management and relevant supervisors may opt to subscribe for notifications on selected events. Thus, all events in this system should contain subscriptions for notifications.

- 6.17.2. Auto-generation of notifications that sent via email or SMS per the law, rules, and regulations to the family, guardian, or relevant staff of MCS dependent on the situation
- 6.17.3. Automatic notifications about changes to the prison status, alert levels, and incidents to stakeholders.

6.18. Prison Incident Management

- 6.18.1. Management of incidents, accidents, and other events inside the prison with history, statements from the relevant inmate, staff, or any other personnel, and binding the incident to the appropriate person's profile.
- 6.18.2. Privileges, if required, are to be cut off in response to incidents.
- 6.18.3. Integration with prison security solution(s)
- 6.18.4. Integration of prison security solutions such as jamming systems, XRAY Machines, Gate/Door Access Systems, and other onsite hardware via SDK or API.

6.19. Prison Conduct

- 6.19.1. Maintain history of events and other activities as conduct
- 6.19.2. Generate reports based on conduct
- 6.19.3. Gather information from other functions of system such as programs and collate to generate a final report that determines the conduct of an inmate.

6.20. Prison Psychological And Counseling

- 6.20.1. Generate schedules and notifications on scheduled and recommended counseling sessions in accordance to the initial psychological assessment.
- 6.20.2. Keep track of sessions and councilors notes.
- 6.20.3. Review triggered assessment reviews.
- 6.20.4. Manage councilor's schedule.

7. PAROLE, CLEMENCY AND OTHER PARDON MANAGEMENT

7.1. Clemency & Parole Board Management

- 7.1.1. Assignment of parole board members, Scheduling of meetings and agendas
- 7.1.2. Storage of Consistent Digital Logs about Decisions made from the meetings.
- 7.1.3. Once the parole board reaches a decision, notification and response from the parole board shall be generated and presented to the inmate.

7.2. Parole Eligibility Calculation and Application

- 7.2.1. Parole Eligibility to be calculated automatically by the software via a dynamic algorithm per the law, rules, and regulations and generation of notifications according to legislation.
- 7.2.2. Management of applications from inmates for parole and tracking its status.
- 7.2.3. Communicating with APIs available from stakeholders to fetch information required.
- 7.2.4. Generation of request for information, and send to stakeholders via email.

7.3. Parole Document management

- 7.3.1. Manage documents related to parole and its statuses.
- 7.3.2. Progress report generation and notifications.

7.4. Monitoring

- 7.4.1. Random schedule for monitoring to be generated amongst the staff present.
- 7.4.2. Log of officer findings and other remarks are to be stored.
- 7.4.3. Failing conditions are to trigger appropriate actions.

7.5. Exceptions and pardons

- 7.5.1. Request for exceptions and pardons

- 7.5.2. Medical related escalations to be logged accordingly and copied in medical module
- 7.5.3. Status tracking of requests
- 7.5.4. History of requests and status

8. HOUSE ARREST AND ISLAND BANISHMENT EXECUTION

8.1. Daily monitoring and officer roster generation

- 8.1.1. Formation of the roster for parole and monitoring officers.
- 8.1.2. Integration with Tracking Equipment
- 8.1.3. Integration of Smart Tags, Location Tracking Devices.

8.2. Escort management

- 8.2.1. Management of notices
- 8.2.2. Management of officers in case of necessary escorts

8.3. Exceptions and pardons

- 8.3.1. Request for exceptions and pardons
- 8.3.2. Medical related escalations to be logged accordingly and copied in medical module
- 8.3.3. Status tracking of requests
- 8.3.4. History of requests and status

8.4. Sentence Execution And Calculation

- 8.4.1. Calculate sentence execution as it happens according to law and provide an interface for relevant institutions and councils to enter data relevant to the execution of the sentence.

8.5. Monitoring And Progress Reports

- 8.5.1. Information about the execution (in case the person is in an island with no MCS personnel) should be uploaded via an interface provided to the relevant council provided by this system

8.6. Islaahu Program For Juveniles

- 8.6.1. Generate duty rosters for officers and other monitoring personnel
- 8.6.2. Manage violation of terms and take actions accordingly.
- 8.6.3. Generate report(s) required for court and other monitoring institutions.
- 8.6.4. Generate progress and status report(s)

9. COMMUNITY SERVICE EXECUTION

9.1. Daily monitoring and officer roster generation

- 9.1.1. Formation of the roster for parole and monitoring officers.
- 9.1.2. Integration with Tracking Equipment
- 9.1.3. Integration of Smart Tags, Location Tracking Devices.

9.2. Escort management

- 9.2.1. Management of notices
- 9.2.2. Management of officers in case of necessary escorts

9.3. Sentence Execution And Calculation

- 9.3.1. Calculate sentence execution as it happens according to law and provide an interface for relevant institutions and councils to enter data relevant to the execution of the sentence.

9.4. Exceptions and pardons

- 9.4.1. Request for exceptions and pardons

- 9.4.2. Medical related escalations to be logged accordingly and copied in medical module
- 9.4.3. Status tracking of requests
- 9.4.4. History of requests and status

[REMAINDER OF THIS PAGE LEFT BLANK INTENTIONALLY]

9.5. Monitoring And Progress Reports

- 9.5.1. Information about the execution (in case the person is in an island with no MCS personnel) should be uploaded via an interface provided to the relevant council provided by this system.

Note: Community service sentence was introduced recently and still is under review by the relevant institutions and the ministry of home affairs at the time this document was written. This component may or may not include further features that have not been discussed in this subheading.

10. REHABILITATION FRAMEWORK MANAGEMENT

10.1. Educational Course Enrolment and Management

- 10.1.1. Management of courses and enrolment of inmates' dependent on eligibility
- 10.1.2. Maintain the attendance of students
- 10.1.3. Grading and report generation
- 10.1.4. Manage violation of terms and take actions accordingly.

10.2. Vocational Training Enrolment and Management

- 10.2.1. Management of vocational opportunities and enrolment of inmate's dependent on eligibility
- 10.2.2. Maintain the attendance of attendees
- 10.2.3. Grading and report generation
- 10.2.4. Manage violation of terms and take actions accordingly.

10.3. Employment Management and Payroll Calculation

- 10.3.1. Management of Enrolment opportunities and enrolment of inmates' dependent on eligibility
- 10.3.2. Maintain the attendance of attendees
- 10.3.3. Payroll and report generation
- 10.3.4. Manage violation of terms and take actions accordingly.

10.4. Community Program Management

- 10.4.1. Manage eligibility dependent on completion of phases and generate notifications accordingly.
- 10.4.2. Provide an interface for associated organizations and other entities to provide data about behavior, attendance and other aspects of the program.
- 10.4.3. Manage history and other information about community programs.
- 10.4.4. Generate status reports to verify compliance with programs.
- 10.4.5. Manage violation of terms and take actions accordingly.

10.5. Management of Program History

- 10.5.1. Use data from initial assessment and other relevant information to determine programs recommended for inmate.
- 10.5.2. Manage history of program completion, attendance and detailed information.

11. CORRECTIONAL FACILITY MANAGEMENT

11.1. Facility Medical Center Management

- 11.1.1. Manage medical centers within the facility similar to that done in medical module.
- 11.1.2. Maintain stock and inventory of medication, consumables and other relevant medical information

11.2. Occurrence

- 11.2.1. Log of occurrence that contains all incidents happening within correctional facility premises.
- 11.2.2. In case of automated systems that provide data, data is to be included in the occurrences.
- 11.2.3. Manual entry of occurrence from officers in the levels of
 - 11.2.3.1. Unit
 - 11.2.3.2. Wing
 - 11.2.3.3. Facility
- 11.2.4. Collation of information provided from levels to generate occurrences in a required duration.

11.3. Asset Management

- 11.3.1. Manage assets utilized in providing services for inmates. (examples: fans, lights pillows)
- 11.3.2. Manage requests and relate them if necessary to grievances, complaints if relevant.
- 11.3.3. Track requests and procuring processes.

11.4. Maintenance Management

- 11.4.1. Generate maintenance requests for prison infrastructure, assets, and other assets.
- 11.4.2. Assign maintenance tasks to teams/staff and others.
- 11.4.3. Track on maintenance progress.

11.5. Prison Status Management

- 11.5.1. Change of prison status with ongoing activities.
- 11.5.2. Generate notifications based on status.

11.6. Duty management

- 11.6.1. Random point of duty generation on selected cells, wings or units.
- 11.6.2. Management of static allocations.
- 11.6.3. History of duty attendance, meal and other breaks
- 11.6.4. Use of integrated door access and other relevant systems into logs.

11.7. Facility Isolation

- 11.7.1. Facilities like juvenile justice unit, female unit, remand units and any other unit mentioned by law, regulation or rules to operate accordingly.
 - 11.7.1.1. Example: Juvenile units do not have privileged of smoking.

11.8. Raids and Riot Management

- 11.8.1. Maintain history of raids, findings, confiscated items and further details as associated regardless of raids being pre scheduled or without prior notice.
- 11.8.2. Maintain officers, inmates related with riots and raids.
- 11.8.3. Track and maintain history of confiscated items and contraband
- 11.8.4. Maintain information about lethal, non-lethal and other actions taken regard to situation.
- 11.8.5. Also relatable to prison incident in prison sentence execution.
- 11.8.6.

11.9. Visitor Registration

- 11.9.1. Generate scheduled visits from relevant organizations and authorities
- 11.9.2. Generate visitor logs and maintain history
- 11.9.3. Communication with door access equipment to provide easy management of access.

12. DOCUMENT MANAGEMENT

12.1. Document Generation

- 12.1.1. Digital Signature with 2FA verification requiring no physical signature.
- 12.1.2. Print Hash Generation that generates A Unique Hash On All Documents printed using the system.
- 12.1.3. All document(s) generated from the system should be available in both “Dhivehi” and “English” language.

[REMAINDER OF THIS PAGE LEFT BLANK INTENTIONALLY]

13. HUMAN RESOURCE MANAGEMENT

13.1. Staff management

- 13.1.1. Management of staff information, leaves, and other related tasks.
- 13.1.2. Integration with attendance monitoring equipment to monitor attendance and provide mediums to view attendance information.
- 13.1.3. Generation of HR related documents such as attendance reports, payroll and other relevant documentation.
- 13.1.4. Management of foreign employees and their work permits and other formalities required by the government of Maldives.
- 13.1.5. Management of different types of staff in accordance to law, rules and regulations.

13.2. Employment and Terminations

- 13.2.1. Manage New Recruits
- 13.2.2. Manage Terminations Of Employees
- 13.2.3. Manage Job Titles And According To Finance Ministry.

13.3. Staff applications

- 13.3.1. Internal method(s) allows staff to check their leave balances and attendance and apply for the human resource department's services.

13.4. Performance evaluation

- 13.4.1. Generate performance evaluation scores depending on the terms and conditions defined in the law, rules, and regulations.
- 13.4.2. Generate and evaluate essential physical examinations (Basic Fitness Tests)
- 13.4.3. Manage The Enrollment for Refreshers and extra training
- 13.4.4. Manage The Enrolment of officers and other staff to courses organized by the institution.

13.5. Employment Rotations

- 13.5.1. Management of rotations that interchanges employees across correction facilities.

13.6. Attendance And Payroll Generation

- 13.6.1. Gather information from attendance machines to integrate with government financial software and communicate to send data required to process financial aspects of payroll.

14. INTELLIGENCE MANAGEMENT

14.1. Intelligence Officer Management

- 14.1.1. Management of the intelligence officers in the system.

14.2. Case management

- 14.2.1. Management of cases dependent on directions and other sources of information.

14.3. Source and Information Management

- 14.3.1. Management of sources and grading based on information.

14.4. Generation of intelligence event/notification without confidential details disclosed for general users.

- 14.4.1. Association of suspects from public, staff, and offenders stored in the system.

[REMAINDER OF THIS PAGE LEFT BLANK INTENTIONALLY]

14.5. Information Evaluation

- 14.5.1. Approval or removal of information by analysts to increase the accuracy of information.

14.6. Collation Of Information

- 14.6.1. Generation of evaluated information for further analysis

14.7. Analysis And Report Generation

- 14.7.1. Generate report(s) based on the collated information and reliable sources.

14.8. Actions

- 14.8.1. Association with predictable events and actions of the related module of this system for further action.
- 14.8.2. Scheduling of raids and other associated functions from the system.

15. CORRECTIONAL INSTITUTE MANAGEMENT

15.1. Document management

- 15.1.1. Management of educational documents that are not in digital form is to be scanned, uploaded, sorted, and managed via the solution in an easy to fetch manner.

15.2. Generation of certifications concerning the completion of courses.

- 15.2.1. Certification validation portal for verification purposes by third parties.

15.3. Course Management

- 15.3.1. Management of modules in courses, enrollments, and generation of transcripts related to courses.
- 15.3.2. Assignment and file uploads
- 15.3.3. Management of handouts, assignments and create an eLearning environment via the solution similar to Google Classrooms
- 15.3.4. Generation of announcements via an online portal
- 15.3.5. Management of course applicants, documents, and other formalities required
- 15.3.6. Attendance and other criteria tracking and management
- 15.3.7. Generation of course completion transcripts, final grading, marking schemes, and other formalities.

15.4. Faculty Management

- 15.4.1. Management of faculties categorized under the institute
- 15.4.2. Generation of event calendar of faculty.
- 15.4.3. Generation of Administrative documents due to submission to educational authorities

15.5. Student Management

- 15.5.1. Management of student profile and histories
- 15.5.2. Management of payments and related financial aspects of courses that require fees.

15.6. Lecturer , Registrar, and trainer management

- 15.6.1. Management of lecturers, trainers, and other personnel concerning courses and additional short training(s).
- 15.6.2. Short pieces of training and assessments

15.7. Announcement and management of participants for short pieces of training

- 15.7.1. Generation of assessment notices and enrollment for assessments concerning the request.
- 15.7.2. Evaluation of assessments and update to human resource or relevant department.

ANNEXURE III

CHANGE REQUEST CONTRACT (CRC)

1. The Change Requests are to be generated on a request basis, and payments are to be made only based on the major changes agreed between the parties.
2. Though there is a CRC that can be used to enhance the system even after the whole implementation, the vendor must use all rational attempts to study the fundamentals of the system thoroughly during the initial implementation period.
3. If there are major change(s) in the requirements of the system, the vendor must provide post-implementation support under a CRC for 1 (one) year from the date of acceptance of the software by MCS.
4. Change Request charges will be estimated in terms of the man-day rate. In the financial proposal, the vendor must submit the man-day rate for each person who will be involved in the change management. The rates should be valid for 1 (one) year. The total cost for the change will be worked out from the quoted rates and the total man days needed to address the changes
5. The man-day rate payable to the vendor, as quoted for the first year, shall be subject to adjustment for the 2nd and 3rd year, taking into consideration the local inflation. The adjustments will be made in accordance with the procurement procedures of GOM.
6. The vendor shall not satisfy frequent changes in the system from the client, once the requirements are finalised. Nevertheless, the changes that come by the change management shall be executed by the vendor under the terms and conditions of the CRC.
7. Whenever there are major new requirements due to a change in the procedures and/or guidelines of the MCB, the client will ask for additional requirements through a Change Request Document. The work involved in the change request and the cost will be worked out by both clients and vendors and a cost will be agreed within the framework of this CRC.
8. The CRC shall be initiated, if the change considered is major, which would have a major impact on the database, the workflow of the system or when there is a major vulnerability found in the system.
9. The minor modifications of fields within an existing form and/or screen or changes having minor or no impact on the database will be addressed as specified in the Warranty Support (more details in the Warranty Support And Maintenance section of this document). The minor changes will not be addressed by the CRC.
10. The vendor will be bound to carry out the CRC made by MCS until 3 years after completion of the implementation. An agreement shall be signed for this contract.

[REMAINDER OF THIS PAGE LEFT BLANK INTENTIONALLY]

ANNEXURE IV

NON-DISCLOSURE AGREEMENT

This agreement is entered into this ___ day of _____, 20__ by and between _____ (hereinafter "Recipient"), with offices at _____, and _____, with offices at _____ (hereinafter "Disclosure"). WHEREAS Disclosure possesses certain ideas and information relating to _____ that is confidential and proprietary to the Disclosure (hereinafter "Confidential Information"); and WHEREAS the Recipient is willing to receive disclosure of the Confidential Information agreeable to the terms of this agreement for the purpose of _____;

NOW THEREFORE, in consideration for the mutual undertakings of the Disclosure and the Recipient under this agreement, the parties agree to the below terms as follows:

1. Disclosure

- 1.1. The Disclosure agrees to disclose, and the Receiver accepts to receive the Confidential Information.

2. Confidentiality

- 2.1. No Use: The Recipient agrees not to use the Confidential Information in any way or manufacture or test any product embodying Confidential Information, except for the purpose approved by the Disclosure.
- 2.2. No Disclosure: The Recipient agrees to use its best efforts to prevent and protect the Confidential Information, or any part thereof, from disclosure to any person other than the Recipient's employees that require disclosure in connection with the Recipient's allowed use of the Confidential Information.
- 2.3. Protection of Secrecy: The Recipient agrees to take all steps reasonably necessary to protect the secrecy of the Confidential Information and to restrict the Confidential Information from falling into the public domain or the possession of unauthorized person(s).

3. Limits on Confidential Information

- 3.1. Confidential information shall not be deemed proprietary, and the Recipient shall have no obligation concerning such information where the information:
- 3.1.1. Was known to the Recipient before receiving any of the Confidential Information from the Disclosure;
- 3.1.2. Has become publicly known due to no wrongful act of the Recipient;
- 3.1.3. Was acquired by the Recipient without breach of this contract from a third party without constraint as to the use and disclosure of the information;
- 3.1.4. Was independently developed by the Recipient without the use of the Confidential Information; or
- 3.1.5. Was directed to be publicly published by the requirement of a government agency.

4. Ownership of Confidential Information

- 4.1. The Recipient agrees that all Confidential Information shall endure the property of Disclosure and that the Disclosure may use such Confidential Information for any purpose without commitment to Recipient. Nothing contained herein shall be interpreted as granting or implying to the Recipient any assignment of rights, any patents, or any other intellectual property about the Confidential Information.

5. Term and Termination

- 5.1. The obligations of this agreement shall be continuing until the Confidential Information revealed to the Recipient is no longer confidential.

6. Survival of Rights and Obligations

This agreement shall be binding upon, inure to the interest of, and be enforceable by (a) the Discloser, its heirs and assignees; and (b) the Recipient, its heirs, and assignees. IN WITNESS WHEREOF, the parties have fulfilled this agreement effective as of the date first written above.

[REMAINDER OF THIS PAGE LEFT BLANK INTENTIONALLY]