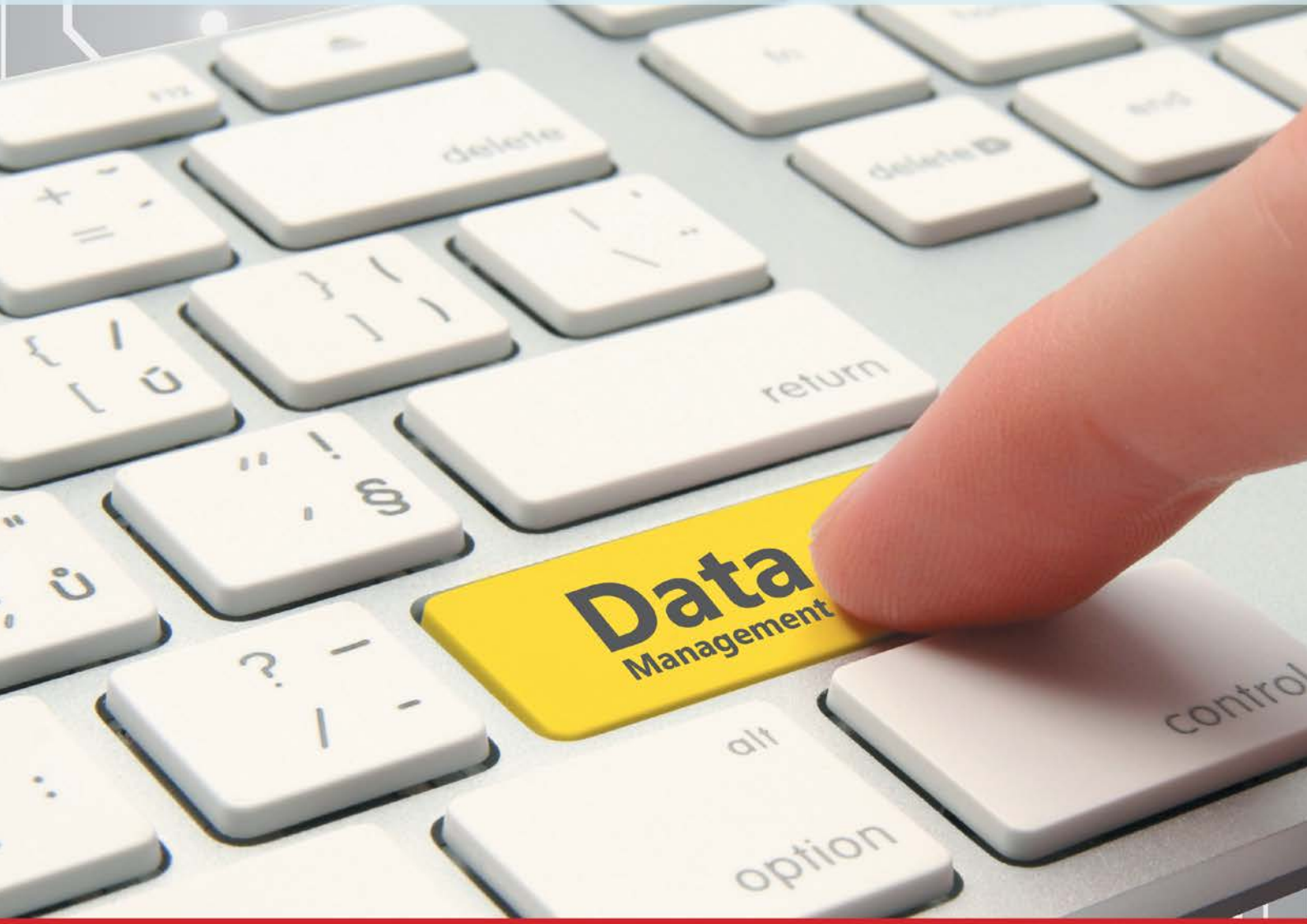
Republic of Mauritius

DATA GOVERNANCE FRAMEWORK

HUMAN RESOURCE MANAGEMENT INFORMATION SYSTEM



Ministry of Civil Service and Administrative Reforms

...for a professional public service committed to excellence

ACRONYMS

DGF …… Data Governance Framework

CISD ……..Central information Systems Division

DPA ……..Data Protection Act

DPO ……Data Protection Office

GINS ……..Government Intranet Network System

HRMIS ……..Human Resource Management Information System

MCSAR ……..Ministry of Civil Service & Administrative Reforms

TAS ……..Treasury Accounting System

TABLE OF CONTENTS

1.0 EXECUTIVE SUMMARY

Data is the most valuable asset of an organization. In order to effectively manage such assets, it is vital for an organization to put in place and implement the right policies and procedures, structures, as well as clear roles and responsibilities. Mismanagement of data leads to inconsistent, inaccurate and unreliable decisions which adversely affect the performance of an organisation.

The Human Resource Management Information System (HRMIS) driven by the Ministry of Civil Service and Administrative Reforms (MCSAR) involves management of human resource and financial data in respect of public officers. The more people are involved in handling the data, the bigger is the challenge to manage the situation. Hence, the need for a formal data governance framework.

Data Governance is the overall management of the availability, usability, integrity, quality, consistency, and confidentiality/security of the data used in an organisation. A Data Governance Framework for the HRMIS will, thus, enable MCSAR to have adequate control over and make good decisions about the use, manipulation, sharing and storage of the data.

This document, therefore, sets the guidelines for all stakeholders concerned with the HRMIS for an effective data management.

The Data Governance Framework is, however, a dynamic document, which can be amended to respond to changing needs of the Civil Service, as to be decided by the Ministry of Civil Service and Administrative Reforms (MCSAR) or the relevant mechanism put in place.

Note:

The rules set out in this document, however, apply exclusively to data used in the context of HRMIS. Non-compliance thereto will undoubtedly affect data integrity which will prove costly to Government and may lead to prosecution under the Data Protection Act or other relevant existing laws of Mauritius.

2.0 INTRODUCTION

2.1 ABOUT HUMAN RESOURCE MANAGEMENT INFORMATION SYSTEM (HRMIS)

The Civil Service has a key role to play to develop Mauritius into a modern and sustainable state with a high standard and quality of life. New and emerging global and local challenges as well as technological development require that the Civil Service continually re-engineers and re-invents itself in order to face those challenges and help the country maintain its competitive edge. It is believed that only a robust Civil Service, duly supported with, inter-alia, a sound human resource management, could help to achieve such vision. Sound human resource management implies judicious and productive utilization of human resources (Talent Management) to ensure that the right person is at the right place at the right time. This calls for synchronized action involving human resource planning, development and management across the Civil Service.

The Integrated Human Resource Management Information System (HRMIS), driven by the Ministry of Civil Service and Administrative Reforms(MCSAR), provides for a single on-line database on public officers to allow Ministries/ Departments to better manage their respective human resources within a modern, re-engineered and less-paper environment.

The integrated HRMIS comprises five Oracle based modules namely: Human Resource, Payroll, Self-Service, Learning Management and Performance Management System. A change carried out to the human resource database would immediately be reflected in all modules. Users of the different modules would thus access the same data/information on a public officer.

Moreover, to facilitate on-line transactions and exchange of reliable HR data for use by different government organisations, HRMIS will interface with the following computerised systems:

(a) The Recruitment System at the Public and Disciplined Forces Service Commissions
(b) The E-Budgeting System at the Ministry of Finance and Economic Development
(c) The Treasury Accounting System (TAS) at the Treasury Department
(d) The Passage and Pensions System at the Treasury Department

(e) The Electronic Attendance System at the Ministry of Civil Service and Administrative Reforms.

3.0 ABOUT DATA

The Data Protection Act (DPA) 2004 has defined data as "*information in a form which is capable of being processed by means of equipment operating automatically in response to instructions given for that purpose; and is recorded with the intent of it being processed by such equipment; or is recorded as part of a relevant filing system or intended to be part of a relevant filing system*".

In line with the Act, the Data Protection Office (DPO) has defined the principles to be observed while dealing with people's data. Every precaution has therefore been taken to adhere to those principles while preparing this document.

3.1 DATA IN THE HRMIS

The implementation of the HRMIS project entails capturing, cleansing, input, safe storage, maintenance, processing and exchange of data ranging from recruitment to retirement of all public officers. To effectively meet its objective, especially as HRMIS will interface with the Treasury Accounting System (TAS) and E-Budgeting, contract officers as well as members of the National Assembly are also covered in the HRMIS.

The HRMIS contains Master Data migrated from the Data Cleansing Application following extraction of data from personal files of public officers recorded on a Data Capture Form.

Apart from basic personal details, HRMIS include data about employment History, payroll, qualifications, and performance details, disciplinary and other records in respect of public officers.

3.2 PRINCIPLES GOVERNING HANDLING OF DATA

Proper processing of data through the HRMIS is a necessary requirement for the effective execution of the contract between the State as the employer and public officers as employees and all those being paid salaries and/or allowances from public funds, including members of the National Assembly. Processing of their data for non-official matters or for personal motive is, therefore, strictly prohibited. Non-compliance to this principle may lead to prosecution under the relevant legislations.

3.2.1 GUIDING PRINCIPLES TO BE OBSERVED BY USERS

The guiding principles to be observed by all users in handling HRMIS data /information are as follows:

- Data should be processed fairly and lawfully.
- Data/information should be obtained only for the specified and lawful purpose and should not be further processed in any manner incompatible with that purpose.
- Data should be adequate, relevant and not excessive in relation to the purpose for which they are processed.
- Data should be accurate and kept up to date.
- Data processed for any purpose should not be kept longer than is necessary. Inactive data should be archived and preserved and dealt with in accordance with legal record retention requirements.
- Data should be processed in accordance with the rights of the employees.
- Appropriate security and organisational measures should be taken against unauthorised or unlawful processing of data and against accidental loss or destruction of data/information, or damage thereto.
- Data/information should not be transferred or disclosed to any unauthorized person or body.

4.0 THE HRMIS DATA GOVERNANCE FRAMEWORK

4.1 THE NEED FOR AN APPROPRIATE FRAMEWORK

The effective implementation of a central computerised system like the HRMIS relies on quality data, hence, the need to have full clarity on data ownership, access, usage, and management. When these are not defined, quality of data gets affected leading to inconsistent situations impacting on organizational decisions and performance. To manage such issues, it is deemed essential that a formal data governance framework be put in place, especially as HRMIS should be a reliable system for the Civil Service.

4.2 AIM OF THE DATA GOVERNANCE FRAMEWORK

The Data Governance Framework (DGF) sets out the policy and rules to ensure proper data management and maintain data integrity, while using the HRMIS. The aim is to guide Users of the system, particularly officers working in the Human Resource and Finance Divisions of Ministries/Departments in effectively carrying out their respective duties while ensuring that organizational data is complete, correct, accurate, consistent and aligned with approved sets of rules and protected as well. It also establishes who is responsible for what under various circumstances, and also specifies the procedures to be followed to deal with specific situations.

5.0 DATA GOVERNANCE DRIVERS

5.1 DATA STAKEHOLDERS

Four groups of stakeholders namely the **Data Steward, Data Controller, Data Custodian and Data User** come into play to support the governance of data in the context of the HRMIS project. Through this framework, MCSAR will be able to exercise positive control over the processes and methods used while handling data.

5.1.1 DATA STEWARD

The Senior Chief Executive, Ministry of Civil Service and Administrative Reforms, is the Data steward, whose main responsibility consists of defining data governance policies and advising Data Controllers and Data Custodians on the implementation of those policies. While overseeing data administration and usage he/she ensures that each assigned data element does not conflict with other data elements and removes both duplicate as well as unused and redundant elements. Where financial data (payroll data) is concerned, the Data Steward consults the Financial Secretary or the Accountant General as appropriate.

5.1.1.1 Data Management Committee

A Data Management Committee, chaired by MCSAR and comprising representatives of the Ministry of Finance and Economic Development (Financial Operations Cadre); Treasury Department; Statistics Mauritius; Pay Research Bureau will from time to time advise the Data Steward on issues like data structure, codification, naming conventions, etc.

5.1.1.2 Data Storage, Back-up and Recovery

The Data Steward defines the rules and procedures to ensure safe data storage in a secured data centre, data back-up and recovery in response to events that could compromise data integrity. In carrying out such responsibility, the Data Steward will stand guided by the existing legal framework and technical advice of the Ministry of Technology, Communication and Innovation, including the Central Information Systems Division, Central Informatics Bureau, IT Security Unit, and the Government On-line Centre.

5.1.2 DATA CONTROLLER

The Data Protection Act (DPA) 2004 defines a Data Controller "*as a person who, either alone or jointly with any other person, makes a decision with regard to the purposes for which and in the manner in which any personal data are, or are to be, processed".*

Given that the day to day management of Human Resources and processing of data in Ministries/Departments falls under the purview of the respective Supervising Officer, the latter is considered to be the Data Controller.

The Data Controller advises the Data Steward on access rights to be made available to members of staff of his/her organisation to perform specific transactions in the HRMIS, for example creation, modification, processing and removal/disposal (archiving) of HR data.

To ensure good data governance at Ministry/Department level, a Data Controller has to put in place such internal control mechanism to ensure that all relevant data sets created or edited in his/her respective organisation conform to the established procedures, norms/standards and conventions as stipulated in this DGF.

5.1.3 DATA CUSTODIAN

An IT officer from the Central Information Systems Division (CISD) is assigned the role of Data Custodian to carry out specific operational responsibilities to ensure the protection of data. The Data Custodian along with the Government On-Line Centre, will look at issues relating to the physical storage, data back-up and assist in the reinforcement of the data management system. In this regard, he/she will have the collaboration of officers of the Central Informatics Bureau and the IT Security Unit regarding the technical controls that have to be put in place to safeguard data. The Government On-Line Centre would provide a seamless service level as per agreement signed with MCSAR. The Data Custodian should

take all the necessary precaution to avoid HRMIS data to be disclosed to or accessed by unauthorized persons/bodies.

5.1.4 DATA USER

Data Users or Users refer to officers at different levels belonging to the HR and Financial Operations Cadres as well as those of General Services who are directly involved in processing and managing (creating, editing, and updating) organizational HR and Payroll/Financial data. Users are bound to understand and follow all specific policies, rules, guidelines and procedures related to the management and protection of data/information, with which they are directly associated and for which they have been given access rights. In this regard, they should be properly briefed and guided by the respective Officers-in-Charge of the HR and/or Finance Divisions, as appropriate. Any violation thereof may result in initiation of appropriate action as per the Data Protection Act (DPA) 2004.

All data Users would be given access rights according to their respective roles and responsibilities, as defined in section 6.0. As regards sensitive data, access would be restricted to a limited number of Users in the HR Division.

6.0 IMPLEMENTATION OF THE HRMIS DATA GOVERNANCE FRAMEWORK

6.1 BASIC PRINCIPLES TO BE OBSERVED

Effective implementation of the Data Governance Framework relies on strict adherence to the basic principles on the part of all stakeholders, especially as the HRMIS will provide on-line information through the Government Intranet Network System (GINS). These are explained below.

6.1.1 DATA INTEGRITY AND TRANSPARENCY

Data Controllers should ensure that employees' data is kept accurate and consistent all the time. In this regard, officers-in-charge of the HR and Finance Divisions would be directly responsible for undertaking such tasks within their respective Divisions. Data emanating from any source and affecting the status of an initial record should always be verified and subject to validation by a different person after input, prior to committing any change in the HRMIS database.

6.1.2 DATA SECURITY

Data security is a way to maintain integrity of data. In spite of the fact that the HRMIS has inbuilt security features, Users have to take all necessary precautions to protect data/information from being accessed by or shared/disclosed to unauthorized persons. Moreover, no User should, by any means, try to access data/information of employees for which no authority has been granted to him/her. Users will thus be able to log onto the HRMIS to access and process only those data/information according to their pre-defined role, which is set, controlled and managed centrally by the Data Steward, with the support of the Data Controller, and where necessary, the Data Management Committee.

6.1.2.1 Accessing the HRMIS System

6.1.2.1 .1 Login Name and Password

All new Users who will be accessing the HRMIS system should fill in 'creation/disabling of User account and access right' template **(Annex A).** Approval for the grant of access rights, "login names and passwords**",** to authorised users falls under the sole responsibility of the Data Steward, upon recommendation of a Data Controller. Such recommendations are subject to scrutiny and may not be totally acceded to for security reasons or where requests are deemed to be excessive. Transactions for the grant of login names and passwords to Users are effected by the System Administrator upon receipt of approval.

6.1.2.1.2 Action upon first login by users

Once a login name and password is received by a User, he/ she should, upon first login, immediately change the password. A strong Password should imperatively contain:

- At least 8 characters.
- At least one special character.
- At least one numeric character.
- A mix of Upper & Lower Case Characters.

Users have only three attempts to login, after which they will not be able to access the System. It is advisable that password be reviewed on a regular basis.

6.1.2.1.3 Change in access rights

Different User groups will be assigned different access rights, based on recommendations made by the Data Controller. All requests for change in access rights should be addressed to MCSAR, using the specified template **(Annex B).** After examination, MCSAR reserves the right to turn down such requests.

6.1.2.1.4 Role of CISD officers in Ministries/Departments

CISD officers based in Ministries/Departments would be empowered to carry out certain tasks e.g. disabling access rights of Users in case of change in posting or schedule of work or transfer to other bodies or resignation/retirement etc. On completion of such transactions, appropriate returns should be made to the Systems Administrator for control purposes.

6.1.3 DATA ACCOUNTABILITY

All Users, Data Controllers and Data Custodians are accountable for their action while handling their respective data/information. Users having given the right to create, edit, amend and delete data should first ensure the correctness thereof prior to validating/committing any transaction in the HRMIS. Correctness of data should always be ensured from official sources/documents. Appropriate internal check mechanism should be put in place at the level of HR and Finance Divisions.

6.1.4 QUALITY ASSURANCE

It is essential that all Ministries/Departments conduct regular preventive internal quality audits to verify the accuracy of their respective data. MCSAR may carry out independent quality audits from time to time.

6.1.5 CHECKS AND BALANCES

The HRMIS provides for checks and balances, whereby the officer performing a transaction should not also be the one validating or confirming such transaction. Officers who have been given the responsibility to verify and validate transactions performed by others should see to it that such tasks are carried out by themselves **personally**. Such responsibility should at no cost be delegated to others. To ensure business continuity, Data Controllers

(Supervising officers in charge of Ministries/Departments) should make appropriate arrangements with the Data Steward (MCSAR) in the event the substantive schedule officer proceeds on leave for either short or long periods. Data Users should not share their login details (username and password) to new users awaiting access rights from MCSAR.

6.1.6 DATA STANDARDISATION

Data being used in the HRMIS has gone through a process of cleansing, formatting, naming and coding, prior to migration therein. Several organisations have accordingly been involved in the exercise to ensure that the HRMIS data structure is aligned with international norms and standards. For example, MCSAR has looked at the job appellation to ensure that they are in line with the Civil Establishment Order; Statistics Mauritius has taken care of all job codes and has enabled alignment with NASCO-8 digits codification; Mauritius Post Ltd assisted in finalizing the format of Residential Address; MoFED /Treasury and MCSAR have synergized to standardize and streamline all Payroll Elements (payments, deductions) – *Allowances having the same meaning but named differently by Ministries/Departments were given the right appellation* ; Salary codes have been aligned to those of PRB and a standard naming convention has been devised for Qualifications.

The appellation structure and format of such data, termed as **Reference Data** have to be maintained. Users having the rights to create and maintain those data should therefore strictly abide by the rules and naming conventions. Any change thereto should follow a change request procedure as indicated at ***Section 6.1.7.1***.

6.1.7 AMENDING DATA

A change process is indispensable to maintain data integrity in the HRMIS. Access to the system will accordingly be strictly controlled and given to a limited number of HR and Finance Staff to make changes to employees' records, particularly because any amendment made to the records of an employee will automatically update the database in the HRMIS.

6.1.7.1 Procedures for amending Reference Data

All amendments relating to Reference Data e.g. salary scale, appellation for jobs, appellation for allowances, allocation of Job Codes, would be centrally carried out by MCSAR. As

regards Reference Data relating to Finance, these would be centrally handled by the Treasury Department.

6.1.7.1.1 Requests for Changes to Reference Data

Requests for changes to Reference Data, where necessary, should therefore be addressed to the Help Desk (HRMIS Unit), MCSAR on the relevant template **(Annex C)** and at the address indicated at ***Section 8.1*****.**

6.1.7.1.2 Reporting of Missing Reference Data

Missing Reference Data should be reported to the HRMIS Unit using the specified template **(Annex C)**.

6.1.7.2 Procedures for amending personal details

Requests received from employees for changes to be made to their personal details e.g. title, surname, address, marital status, contact details and qualifications, should be processed by the authorised staff of the HR Division only.

Requests for changes should be made officially to the Officer-in-charge of the HR Division, either by mail or letter, duly supported by documentary evidence, where appropriate. Records of such request should be kept by the HR Division. This condition also applies to Users of HRMIS having the rights to create, modify records.

Note: No User or employee is allowed to amend his/her own record. The HRMIS has an in-built **Audit Trail System** that will enable the Ministry to get the history of a transaction done on the system.

6.2 DATA SHARING

Subject to there being no legal restriction, Data Controllers may authorize sharing of data of their respective employees to institutions like the Police Department, Judiciary and the Service Commissions or other authorities for specific legal purposes e.g. Appointment, Promotion, Disciplinary Cases, Investigations and Enquiries.

7.0 SOME PRACTICAL SECURITY GUIDELINES FOR USERS OF HRMIS

- Login details (username and password) should under no circumstances be shared among Users or with unauthorised persons.
- In case of a change in posting or schedule of work, access rights of the user/s need to be immediately disabled by the Administrator.
- Relevant changes/adjustment should immediately be made whenever any member of staff changes posting or takes employment elsewhere.
- After a period of inactivity, ensure that computers using the HRMIS are logged off or 'locked' when left unattended for any period of time.
- Ensure that computers are securely locked away from unauthorised people.
- Before leaving office, ensure that computers using HRMIS are logged out and switched off.

8.0 USER SUPPORT/HELP DESK AT MCSAR

8.1 HRMIS UNIT

MCSAR has put in place an HRMIS Unit to guide Users on the proper and effective use of the system. Relevant template has been designed to report specific problem while accessing/using the system **(Annex D).** Officers of the unit may be contacted on 405 4100 (PABX) or 405 5770/71/72/73 or by mail on **hrmisunit@govmu.org.**

8.2 IT UNIT

Similarly the IT Unit of MCSAR headed by the System Administrator, may be contacted on 405 4100 (PABX) or 405 4114 using the template at **(Annex D)**, for all IT related technical issues linked to e.g. Login name; Password and Access Rights, connection with HRMIS, slowness of system.

Note: All requests received from Data Controllers and action taken by the HRMIS or IT Unit will be kept in an appropriate Register.

9.0 TEMPLATES

All issues related to the HRMIS system should be reported to the HRMIS Unit using the following templates:

1.	Creation and Disabling of User Account and Access Rights Template ***(Annex A)***	To request for access to the System and to disable a User Account. (*A User account must be set active/or inactive and must not be deleted.)*
2.	Change of Access Rights Template ***(Annex B)***	To request for change in access rights to the System.
3.	Amendments in Reference Data Template/ Reporting Missing Reference Data ***(Annex C)***	To report to the HRMIS Unit any change in Reference Data and any missing Reference Data in the HRMIS (*e.g. Job references, qualifications)*.
4.	Problem Reporting Template ***(Annex D)***	To report issues related to the System when being accessed/ used.

Note: In no circumstances should a User in any Ministry/Department, including Users in MCSAR, deal directly with the supplier of the System (State Informatics Limited) and/or the Government On-line Centre. Problems should be addressed to the appropriate unit (HRMIS or IT Unit) at MCSAR, as indicated above.

10.0 AMENDMENT TO THIS DGF

This DGF was adopted by the HRMIS Steering Committee on 19 November 2015 (after legal vetting by the Solicitor General's Office and DPO). Any change thereto would need the approval of the Steering Committee or MCSAR, should the former be no longer operational.

APPENDICES

CREATION/DISABLING OF USER ACCOUNT AND ACCESS RIGHTS TEMPLATE - ANNEX A (*This form is to be filled in and signed by the OIC HR or Finance as appropriate)*		
Please tick the relevant box:	**Creation of User Account** ☐	**Disabling of User Account** ☐
PARTICULARS OF NEW/EXISTING USER		
NAME		
GRADE		
MINISTRY/DEPARTMENT		
ACCESS RIGHT LEVEL ***(please tick as appropriate)***	**HR USER** ☐	**HR SUPERVISOR** ☐
MODULES ***(Please list as appropriate)***		
REASON FOR REQUEST		
DURATION		
AUTHORISED BY ***(TO BE SIGNED BY OIC HR OR FINANCE)***		
NAME: **SIGNATURE:**	**GRADE:** **DATE:**	
ACTION TAKEN BY (MCSAR)		
NAME: **SIGNATURE:**	**GRADE:** **DATE:**	

CHANGE OF ACCESS RIGHT - ANNEX B (*This form is to be filled in and signed by the OIC HR or Finance as appropriate)*		
MINISTRY/DEPARTMENT		
PARTICULARS OF USER		
NAME		
GRADE		
SECTION		
CHANGE OF ACCESS RIGHT		
ACCESS RIGHT LEVEL	**FROM …….**	**TO …….**
MODULES		
REASON FOR REQUEST		
DURATION		
AUTHORISED BY *(TO BE SIGNED BY OIC HR OR FINANCE)*		
NAME: **SIGNATURE:**		**GRADE:** **DATE:**
ACTION TAKEN BY (MCSAR)		
NAME: **SIGNATURE:**		**GRADE:** **DATE:**

REQUEST FOR CHANGE/REPORTING MISSING REFERENCE DATA - ANNEX C (*This form is to be filled in and signed by the OIC HR or Finance as appropriate)*	
MINISTRY/DEPARTMENT	
CHANGE IN REFERENCE DATA	
MODULE:	**FIELD NAME:**
PRESENT APPELLATION:	**PROPOSED APPELLATION:**
REASON FOR REQUEST : ***(to attach documentary evidence)***	
MISSING REFEERENCE DATA	
MODULE:	**FIELD NAME:**
PROPOSED APPELLATION:	
REASON FOR REQUEST: ***(to attach documentary evidence)***	
SUBMITTED BY *(TO BE SIGNED BY OIC HR OR FINANCE)*	
NAME: **SIGNATURE:**	**GRADE:** **DATE:**
ACTION TAKEN BY (MCSAR)	
DESCRIPTION OF INTERVENTION MADE:	
NAME: **SIGNATURE:**	**GRADE:** **DATE:**

PROBLEM REPORTING TEMPLATE - ANNEX D			
MINISTRY/DEPARTMENT			
PROBLEM ***(PLEASE TICK AS APPROPRIATE)***			
ACCESS ISSUES: ☐		**SYSTEM ISSUES:** ☐	
DESCIPTION OF PROBLEM ***(to give error message if applicable)*** **:**			
PROPOSED REMEDIAL ACTION ***(if any)*****:**			
REMARKS :			
SUBMITTED BY ***(TO BE SIGNED BY OIC HR OR FINANCE)***			
NAME: **SIGNATURE:**		**GRADE:** **DATE:**	
ACTION TAKEN BY (MCSAR)			
INTERVENTION MADE			
OUTCOME (fixed, pending, etc.)			
ANY OTHER REMARKS			
NAME: **SIGNATURE:**		**GRADE:** **DATE:**	

NOTE:

Ministry of Civil Service and Administrative Reforms
HUMAN RESOURCE MANAGEMENT INFORMATION SYSTEM UNIT
Level 5, SICOM Building 2, Corner Chevreau & Rev Jean Lebrun Streets,
Port Louis, Republic of Mauritius
Tel: *PABX:* 405 4100 (*Ext:* 10044-10047, 10052-10064), Fax: 212 4160
Email: hrmisunit@govmu.org
Website: http://civilservice.govmu.org

Printed by the Government Printing Department (November 2016)