FMIS ACCESS
AND PASSWORD POLICY

Financial Policy Assurance Unit
Ministry of Finance
Ro Lalabalavu House
SUVA

February 2015

FMIS ACCESS AND PASSWORD POLICY

1.0 Introduction

1.1 The FMIS (Financial Management Information System) Access and Password Policy has been formulated to act as a procedural guide to Ministries and Departments in providing clear direction for creation, alteration and disabling of FMIS user privileges.

1.2 The intention is to emphasize the need of proper internal control procedures that would need to be adhered to ensure minimal risk exposure to Government.

2.0 Scope

2.1 This policy applies to all Government officers who have direct and/or indirect access to the FMIS for verification/inquiries, standard order entry, authorization/approval, receiving, invoicing and other processes which require the usage of password to undertake certain financial transactions in the FMIS.

3.0 Purpose

3.1 The purpose of this policy is to:

i) Ensure that all FMIS users understand the importance of passwords and their respective access and should not be used in a manner which is unethical and contradictive to Financial processes and procedures as documented in the Finance Instructions (FI) and the respective Agency Finance Manuals;

ii) Ensure that proper processes are understood and followed in instances whereby users are created, altered or disabled; and

iii) Emphasizing the need to uphold and maintain proper internal controls as well as ensuring accountability in all aspects of the FMIS.

4.0 Definitions

4.1 Director FMIS – the designation of the officer in charge of the Financial Management Information System Unit or given the responsibilities of the position in his/her absence.

FMIS Administrator Helpdesk – the FMIS IT officer within FMIS/MoF to manage the FMIS (mailto: FMIS-AdministratorHelpdesk@govnet.gov.fj)

4.2 FMIS/FMR Staff – The respective module leads in the FMIS Unit (mailto: FMIS-Staff@govnet.gov.fj)

4.3 Module – These are the FMIS system applications such as General Ledger (GL), Accounts Payable (AP), Accounts Receivable (AR), Purchasing Order (PO), Fixed Assets (FA) and Fund Accounting.

4.4 Master Security – FMIS Administrator/ Info Global Consultants

4.5 User – any officer that has been approved by his/her Accounting Head and FMIS/MoF to be given access to the FMIS.

4.6 Panel – FMIS work unit.

5.0 Requirements of the Finance Instructions

5.1 FI 13 states that all system generated purchase orders, indents and other commitments of funds must be recorded in the financial management information system …. after they have been approved.

5.2 FI 20-(7) states that every revenue collector who receives public money, other money or trust money must record the details…..in the financial management information system.

5.3 The respective Agency Finance Manuals also emphasize the usage of the FMIS in the recording and extraction of financial data in the formulation of reports to Management and key users.

6.0 Request for Creation of New FMIS Users Access/ Requests for Panels and Modules

6.1 Prior to requesting creation of new accounts or request for new access to panels and modules, the Accounting Head must ensure that the user has a valid GOVNET Account.

6.2 The Accounting Head must also scrutinize the request and ensure that the User's existing/current access will not contradict any internal control principles and ensure separations of duties are maintained.

6.3 All new users will need to fill in FMIS Access Request Forms (Appendix 2) which will need to be endorsed by their Accounting Head prior to being submitted to FMIS/FMR Staff for consideration. These forms will need to be scanned and emailed by the Accounting Head to FMIS Administrator Helpdesk. Upon decision of request for access, the Accounting Head should also request for a scanned approved/disapproved form for filing.

6.4 It is imperative that proper FMIS Account Forms be filled and requested access for specific panels and/or modules be clearly detailed out in the forms prior to endorsement by the Accounting Head. The Accounting Head may also make reference to the detailed template that may be provided by FMIS Administrator Helpdesk to review Staff access (Appendix 2 provides an example). The FMIS/FMR Staff have the right to refuse acceptance of forms which are incomplete or not clearly detailed out.

6.5 The forms will be vetted by the FMIS Module Leads prior to recommending approval or disapproval of access to Director FMIS.

6.6 All password resets, account activation and deactivation requests must come through the respective Accounting Head to FMIS Administrator Helpdesk by emailing a scanned copy of the request.

6.7 Upon the absence of the Accounting Head to request for creation of new users, password request or account activation/ deactivation, the immediate supervisor (or someone of higher position) of the Accounting Head shall be the officer responsible for requesting for creation of new users, password request or account activation.

6.8 The final decision of creating a new FMIS user account or additional access to panels rests with the Director FMIS on consultation with the module leads.

6.9 At the end of each quarter, the Accounting Head must review the list of active and inactive users and update FMIS/FMR Staff on changes that may need to be made on their respective profiles. Therefore, should a user resign, be terminated, transferred or promoted to a different Ministry, the Accounting Head must inform FMIS accordingly of such changes.

6.10 Upon any request, the Accounting Head must ensure that a soft copy of the request form is made; soft copy to be sent to FMIS Administrator Helpdesk and the hard copy to be retained by the Agency for filing. The Secretary to Director FMIS will be responsible for filing all request forms submitted to FMIS unit and all Accounting Heads are also required to appoint an officer to file all request forms in their respective department/ministries. The Secretary to Director FMIS will also be responsible for updating the ‘FMIS Access Request Register’ as and when request forms reach her.

6.11 The Accounting Head must ensure that all request forms are filed in 6.10 in an appropriate folder and ensure that the data on all FMIS users for the respective Agency is kept up to date for audit purposes.

6.12 FMIS unit will be monitoring all user access on a quarterly basis.

6.13 **Auditors to audit the user access as per requirement of the FMIS Access and Password Policy.**

7.0 Temporary Access

7.1 There may be a situation where temporary access will be required in instances where the Accounting Head or Panel/Module users is/are on leave. In these instances, it is imperative that Accounting Heads make prior arrangements with FMIS one week in advance if leave is anticipated.

7.2 Should the leave of the accounting head or panel or module user is unexpected, arrangements could also be undertaken with Director FMIS by the immediate supervisor of the Accounting Head on the day of the request.

7.3 In either situation 7.1 or 7.2, temporary access may be allowed to users requesting for access. However, the request will need to be on official memo from the requesting Ministry/Department.

7.4 FMIS Administrator Helpdesk with the approval of Director FMIS has the right to deactivate the accounting head’s or any other users (who may be absent) access upon request for temporary access to other users until such time that the accounting head or the user that will be on leave resumes work.

7.5 In relation to temporary increase of approval limits, requests will be subject to Director FMIS approval and will be active for 30 minutes upon which Ministries/Departments must carry out respective clearance of PO's. Upon expiry of the 30 minute time frame, PO Module Lead will deactivate this temporary access.

7.6 **Accounting Heads must ensure that FMIS/FMR Staff are updated and informed on the removal of temporary access given to another user once the responsible officer resumes duties.**

8.0 Processes and Procedures

The internal control minimum and standard criteria for awarding access to different categories of ministries and departments are documented in Appendix 2 Table 1 and 2.

8.1 AP Processes

8.1.1 The segregation of processes in the AP module should ideally be as follows:

a) Vendor creation and amendments are access only by Accounting Heads and/or senior AP officers no one else (AP 131);
b) Raising of vouchers and releasing of vouchers (AP300, 305, 315, 350);
c) Payment selection of vouchers for payments and printing of cash requirement reports (AP401, 410, 415 416);
d) Payment Run (AP419);
e) Cheque Matching (AP467);
f) Payment Acceptance (AP419); and
g) GL scheduling that is given to GL clerk and/or Accounting Head (GL350).

8.1.2 No user should have all the accesses in the AP processes with the exceptions of Accounting Heads;

8.1.3 No user should have accesses to process a, b and c;

8.1.4 No user should have accesses to process a with the other processes.

8.2 PO Processes

8.2.1 The four (4) major processes under the PO Module are:

i) Standard Order Entry (PO401);
ii) Approval (PO348);
iii) Receiving (PO481); and
iv) Invoicing (PO621)

8.2.2 PO Access is to be determined by the Accounting Head of respective Ministries /Departments.

8.2.3 No PO Approver should have access to (i), (iii) and (iv).

8.2.4 A PO Buyer should have access to (i), (iii) and (iv) or be limited to access only 1 process.

8.2.5 Appointments of PO Approvers and approval limits to be made only by the Accounting Head under the authority of the PS.

8.2.6 Appointments of PO Buyers to be made by the Accounting Head.

8.2.7 The request to increase approval limits are to only be made by the Accounting head together with relevant supporting documents.

8.2.8 All appointments, changes, requests and inactivation of accesses are to be facilitated by the use of the FMIS User Access Request Form submitted in writing or emailed to the Director FMIS.

8.2.9 Copies of appointments and requests are to be filed by the Ministries/Departments for documentation and auditing purposes.

8.3 AR Processes

8.3.1 Ideally there are 4 processes under the AR Module

i) Adding of Customers (AR105);
ii) Invoicing (AR411, 526, 550;
iii) Receipting (AR623, 641);
iv) Scheduling of AR batches in GL350

8.3.2 AR access is determined by the respective Ministries and Departments Accounting Heads

8.3.3 No user should have all the accesses in the AR process.

9.0 FMIS Password

9.1 Each User will be assigned a password to access the FMIS.

9.2 The FMIS Administrator Helpdesk must not reveal the initial password of the user to anyone else except the user.

9.3 The Password must be a fixed length of eight alpha numerical characters (mixture of letters and numbers) e.g. DAVID001.

9.4 First time user of the FMIS will be asked to change his/her password upon first login.

9.5 Users who have forgotten their passwords may ask for their password to be reset through email from their Accounting Head to the FMIS Administrator Helpdesk.

The FMIS Administrator Helpdesk has the right to query and clarify identification of the user should the need arise.

9.6 It is necessary that in 9.5 above, the respective form will need to be filled out and submitted to FMR/FMIS Staff for approval. The softcopy of the form is to be emailed to FMIS Administrator Helpdesk for approval. Once approved, FMIS Administrator Helpdesk will notify the decision to the Accounting Head over email. All endorsed forms are to be filed with the Director FMIS's Secretary. Agencies may request a copy for their records from her.

9.7 New passwords will only be sent on users valid GOVNET Email Account.

9.8 The validity of the FMIS passwords is 90 days and since the system prompts for password change, users must change their respective passwords when prompted to do so.

10.0 Request for User Access Account Alteration

10.1 In instances where there is a need to alter/modify user privileges or access, the change of FMIS Access Request form is to be filled by the user in question. The request form is to be scanned and emailed to FMIS Administrator Helpdesk by the Accounting Head.

10.2 The Accounting Head must ensure that prior to considering user privileges or access to users, the user must fit the criteria for those who may be allowed access. The basic criteria will include the following:

- User to have a valid GOVNET account;
- User must be a Permanent or Contracted Government employee (attachees will not be considered for FMIS access);
- User must be well versed with the FMIS Access & Password policy & Govnet Email/Password policy;
- Users must be responsible, honest and trust worthy officers; and
- Basic IT skills in the use of Office Application and Internet web browsing.

10.3 Proper justification for change must be made by the Accounting Head prior to endorsing the form and submitting it to FMIS Administrator Helpdesk.

10.4 The FMIS Administrator must consult the FMR/FMIS Staff prior to implementing any alteration/modification request with the approval of Director FMIS.

11.0 Responsibilities of the Director FMIS

11.1 The Director FMIS shall approve and disapprove all requests for FMIS Access addition or alteration as endorsed by the Accounting Head prior to assessment by the FMIS Module Leads and the FMIS Administrator Helpdesk.

11.2 Director FMIS will make the final decision on whether or not to create a new FMIS user account or to give additional access to panels.

11.3 FMIS Administrator, with the approval of Director FMIS, has the right to deactivate and activate user accounts for temporary access as well as alter FMIS user privileges.

11.4 FMIS Administrator is responsible for nominating a password for a user that requests for access upon approval from Director FMIS.

11.5 Director FMIS upon the recommendation of Module Leads and FMIS Administrator may also liaise with ITC Services on the removal of Govnet privileges to officers found to be breaching the Govnet Email/Password Policy.

12.0 Responsibilities of the FMIS Module Leads

12.1 FMIS Module Leads provide recommendations and advice to the Director FMIS on the approval and disapproval of access request forms endorsed and submitted by the respective Accounting Heads.

12.2 FMIS Module Leads are also responsible for consulting the Accounting Heads and users before recommending any new or additional access.

13.0 Responsibilities of the FMIS Administrator Helpdesk/ Master Security

13.1 The FMIS Administrator is responsible for activating and deactivating all forms of access in the system based on the advice of the Accounting Heads, FMIS Module Leads and approval of Director FMIS.

14.0 Responsibilities of the Permanent Secretary

14.1 The responsibility of respective Permanent Secretaries and Heads of Departments is to approve LPOs online within the prescribed limit.

14.2 Permanent Secretaries and Heads of Departments provided with password /access to FMIS must ensure security of password and must not request any other officer to access the system and approve PO's on his/her behalf.

14.3 Permanent Secretaries must not divulge FMIS access Password to any other officer that he/she may see fit.

15.0 Responsibilities of Deputy Secretaries

15.1 Deputy Secretaries are also responsible for approving LPOs online within the prescribed limit including at any time, being given the position of Acting on Permanent Secretary Positions.

15.2 Deputy Secretaries when provided with FMIS Access Password must not divulge this information with any other officer and must ensure that he/she is solely responsible for approving LPOs online in accordance to the stipulated limit.

15.3 Deputy Secretaries are not allowed to request other officers/subordinates to approve LPOs on his/her behalf.

16.0 Responsibilities of Directors

16.1 Directors are also provided procurement limits and may procure goods and services to a certain amount.

16.1 Directors, when provided with FMIS Access Password, must not divulge this information to any other officer and must ensure that he/she is solely responsible for approve LPOs online in accordance with the stipulated limit.

16.2 Directors are not allowed to request other officers/subordinates to approve LPOs on his/her behalf.

17.0 Responsibilities of FMIS Users

17.1 The responsibilities of FMIS Users are to thoroughly understand the importance of being given particularly access in the FMIS.

17.2 FMIS Users must therefore use the FMIS in accordance with the approved access that has been given to him/her.

17.3 FMIS users must not sign into or attempt to sign into any other users FMIS user account rather than his/her user account.

17.4 FMIS users must not divulge his/her FMIS user access password to anyone.

17.5 FMIS users must use the FMIS in accordance with manner prescribed in the FMIS Access and Password Policy.

18.0 Responsibilities of the Accounting Head

18.1 The Accounting Head must carry out proper awareness to all their respective FMIS users on the importance and significance of FMIS passwords and the need to ensure that security and sharing of passwords is prohibited.

18.2 The Accounting Head is also responsible for checking that a user does not have access to two or more modules/panels[1] that may instigate possible fraud, collusion and breaches of internal control processes.

18.3 The Accounting Head must therefore scrutinize all FMIS access request forms properly and effectively to ensure that (i) the user fits the criteria as listed in 10.2; (ii) details are correct; and (iii) right panels/modules are being applied for prior to endorsing the forms and submitting it to the Director FMIS.

18.4 The Accounting Head must monitor all FMIS users and any changes to the users in terms of new addition and/or deactivation through termination, resignation of staff will have to be updated on quarterly basis to FMIS/FMR Helpdesk as per template provided by the FMR Helpdesk Administrator. (Sample Template is exhibited in Appendix 2; full excel template available with FMR Helpdesk Administrator).The Accounting Head must ensure that all FMIS access request forms submitted to FMIS whether approved or not are to be filed.

19.0 Penalties and Corrective Action

19.1 Users found to be violating the policy causing misuse through unauthorized expenditure, illegal transactions and/or deliberate fraud, may be subject to disciplinary/surcharge action and termination of FMIS/Govnet user account privileges.

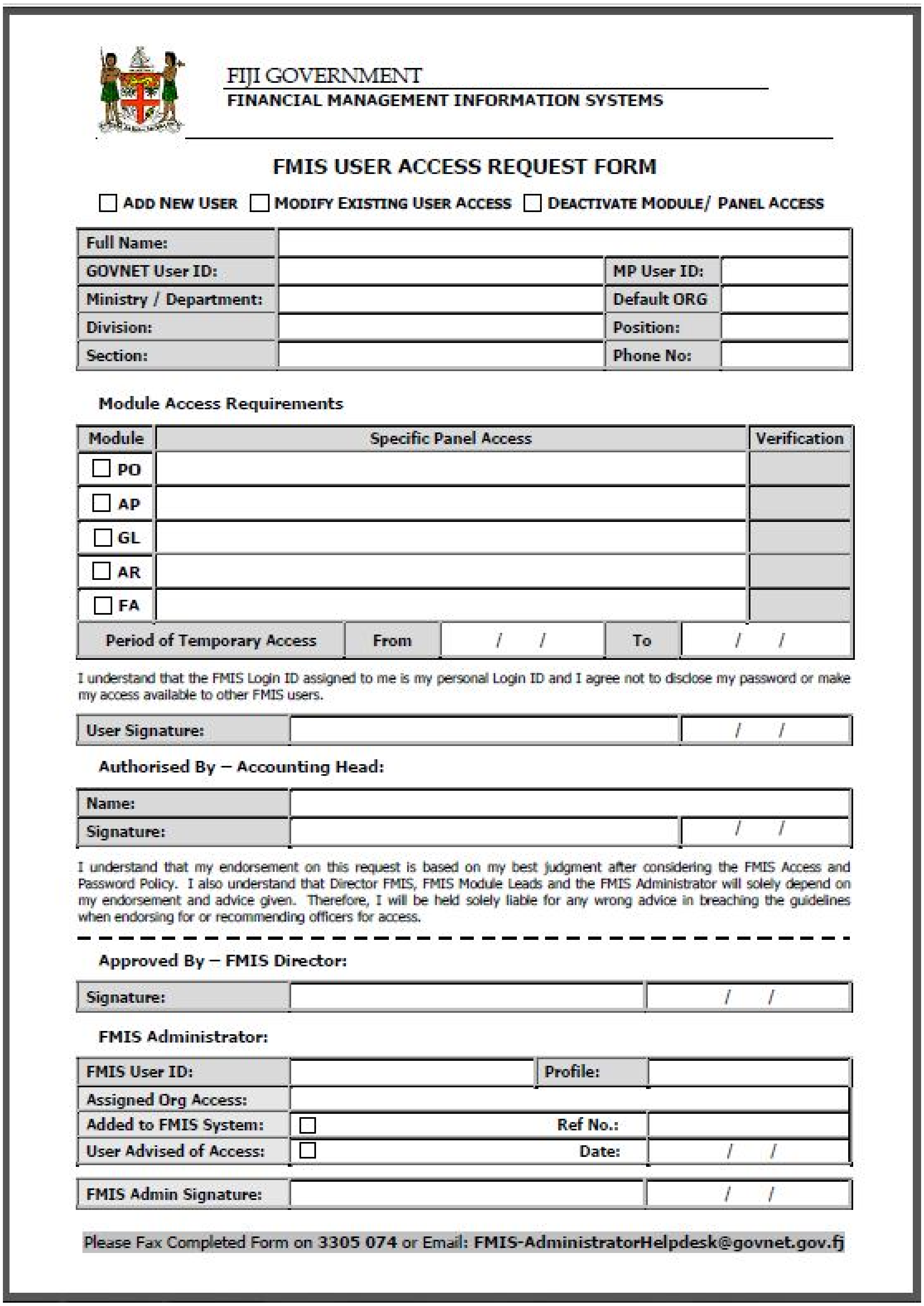
19.2 It must be noted that the Accounting Head maybe held liable for surcharge upon any breaches to the Policy.

20.0 Review

20.0 The Permanent Secretary for Finance may, on the advice of the Financial Policy Assurance Unit review the policy as and when deemed necessary.

Financial Policy Assurance Unit
Financial & Asset Management Division
Ministry of Finance
Ro Lalabalavu House

APPENDIX 1



FIJI GOVERNMENT
FINANCIAL MANAGEMENT INFORMATION SYSTEMS

FMIS USER ACCESS REQUEST FORM

□ ADD NEW USER □ MODIFY EXISTING USER ACCESS □ DEACTIVATE MODULE/ PANEL ACCESS

Full Name:			
GOVNET User ID:		MP User ID:	
Ministry / Department:		Default ORG	
Division:		Position:	
Section:		Phone No:	

Module Access Requirements

Module	Specific Panel Access	Verification
□ PO		
□ AP		
□ GL		
□ AR		
□ FA		

Period of Temporary Access	From	/ /	To	/ /

I understand that the FMIS Login ID assigned to me is my personal Login ID and I agree not to disclose my password or make my access available to other FMIS users.

User Signature:		/ /

Authorised By – Accounting Head:

Name:		
Signature:		/ /

I understand that my endorsement on this request is based on my best judgment after considering the FMIS Access and Password Policy. I also understand that Director FMIS, FMIS Module Leads and the FMIS Administrator will solely depend on my endorsement and advice given. Therefore, I will be held solely liable for any wrong advice in breaching the guidelines when endorsing for or recommending officers for access.

Approved By – FMIS Director:

Signature:		/ /

FMIS Administrator:

FMIS User ID:		Profile:	
Assigned Org Access:			
Added to FMIS System:	□	Ref No.:	
User Advised of Access:	□	Date:	/ /

FMIS Admin Signature:		/ /

Please Fax Completed Form on 3305 074 or Email: FMIS-AdministratorHelpdesk@govnet.gov.fj

APPENDIX 2

For the purpose of this policy the category/criteria of ministries and departments in terms of size are dependent on the number of accounts personnel in that particular ministry/department as documented in Table 1. (Should this be included under s.4.0: Definitions?)

Table 1

	CATEGORY OF MINISTRY/DEPARTMENT		
Size of Ministry/Department	SMALL	MEDIUM	LARGE
Number of Accounts Personnel	Maximum of 2 Officers	Maximum of 3 Officers	4 or More Officers

The internal control standard and basic criteria for awarding access for functional sub modules namely Purchase Order, Accounts Payable and Accounts Receivable are documented in Table 2. (To be included in s.8)

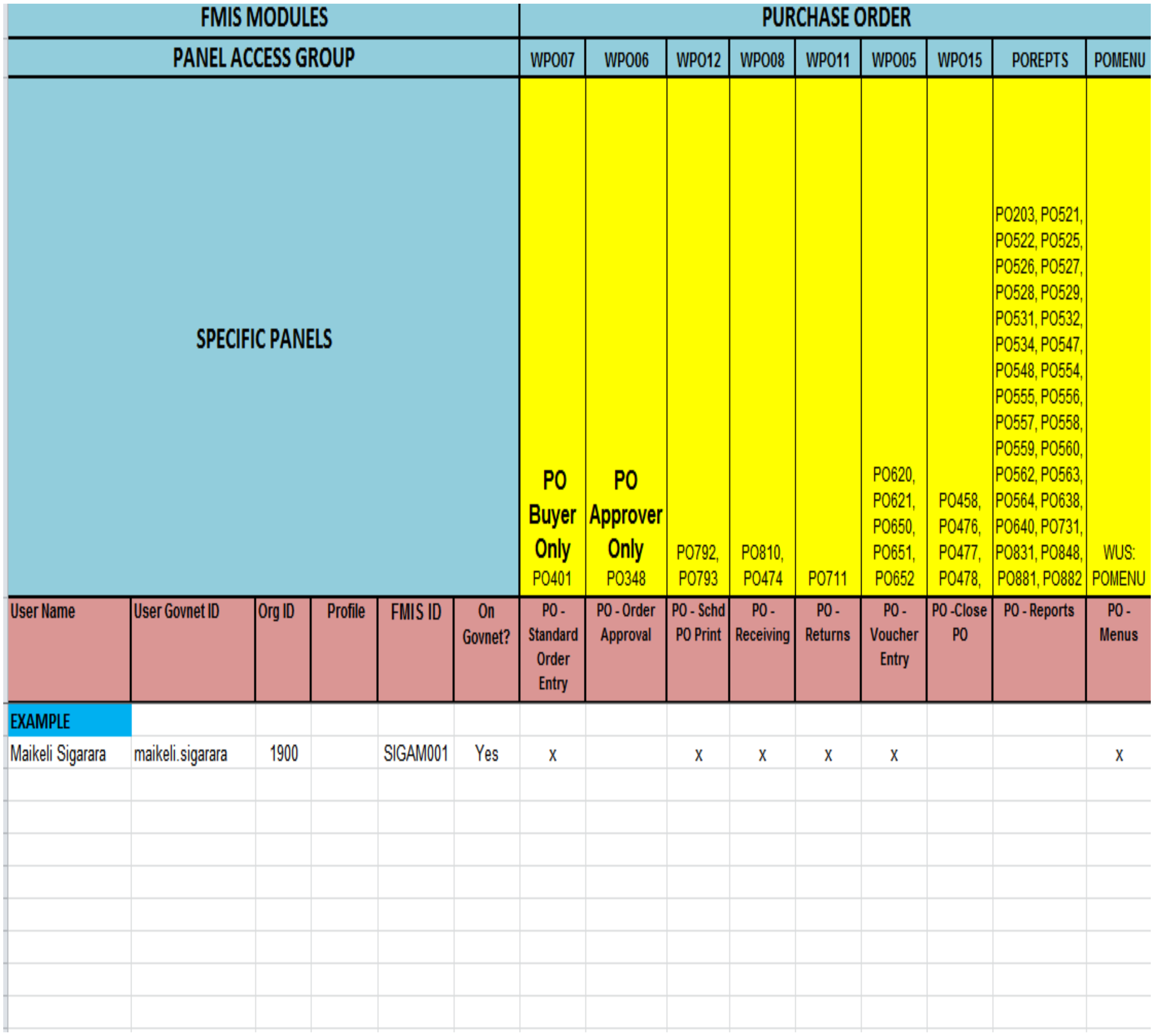
Table 2

MODULE	**Number of Officers**	**CATEGORY OF MINISTRY/DEPARTMENT**		
		SMALL	MEDIUM	LARGE
PURCHASE ORDER (PO)	1	i. Create PO ii. Receive PO iii. Invoice PO	i. Create PO	i. Create PO
	2	i. Approve PO	i. Approve PO	i. Approve PO
	3		i. Receive PO ii. Invoice PO	i. Receive PO
	4			i. Invoice PO
ACCOUNTS PAYABLE (AP)	1	i. Vendor Creation ii. Schedule GL350	i. Vendor Creation ii. Schedule GL350	i. Vendor Creation ii. Schedule GL350
	2	i. Vouchering ii. Payment Selection iii. Payment Run iv. Cheque Matching v. Payment Acceptance	i. Vouchering	i. Vouchering
	3		i. Payment Selection ii. Payment Run iii. Cheque Matching iv. Payment Acceptance	i. Payment Selection
	4			i. Payment Run ii. Cheque Matching iii. Payment Acceptance

ACCOUNTS RECEIVALBE (AR)	1	i. Adding of Customers ii. Schedule GL 350	i. Adding of Customers ii. Schedule GL 350	i. Adding of Customers ii .Schedule GL 350
	2	i. Invoicing ii. Receipting	i. Invoicing	i. Invoicing
	3		i. Receipting	I .Receipting

APPENDIX 3

Example of PO User Details



FMIS MODULES						PURCHASE ORDER								
PANEL ACCESS GROUP						WPO07	WPO06	WPO12	WPO08	WPO11	WPO05	WPO15	POREPTS	POMENU
SPECIFIC PANELS						PO Buyer Only PO401	PO Approver Only PO348	PO792, PO793	PO810, PO474	PO711	PO620, PO621, PO650, PO651, PO652	PO458, PO476, PO477, PO478,	PO203, PO521, PO522, PO525, PO526, PO527, PO528, PO529, PO531, PO532, PO534, PO547, PO548, PO554, PO555, PO556, PO557, PO558, PO559, PO560, PO562, PO563, PO564, PO638, PO640, PO731, PO831, PO848, PO881, PO882	WUS: POMENU
User Name	User Govnet ID	Org ID	Profile	FMIS ID	On Govnet?	PO - Standard Order Entry	PO - Order Approval	PO - Schd PO Print	PO - Receiving	PO - Returns	PO - Voucher Entry	PO -Close PO	PO - Reports	PO - Menus
EXAMPLE														
Maikeli Sigarara	maikeli.sigarara	1900		SIGAM001	Yes	x		x	x	x	x			x