Ministry of Agriculture

Republic of Liberia

Subject: **Policy on the Acceptable Usage of ICT Resources**

DOCUMENT CONTROL

Document Name	**Draft Policy on the Acceptable Usage of ICT Resources – Programme Management Unit/Ministry of Agriculture, Liberia**
Language(s)	English
Responsible Unit	The Ministry of Agriculture ICT Department and out posted offices
Creator (individual)	Johnson S. Chelleh/ICT Specialist (PMU/MOA)
Subject (taxonomy)	Information Technology Management/Technical Services/Policy on the acceptable usage of ICT Resources
Date Created	June 2015
Date Updated	June 2015
Mandatory Review	(12 months past publish date)
Audience	All PMU/MOA staff using ICT resources owned or operated by the PMU/MOA and out posted offices
Applicability	All individuals accessing the PMU/MOA and out posted offices ICT resources

Date	Author	Version	Change Reference
10/06/2015	Johnson S. Chelleh	1.0	June 2015
20/06/2016	Johnson S. Chelleh	1.1	June 2016

Table of Contents

General Statement

This policy document on acceptable usage of ICT Resources comprises a variety of systems that handle electronically retrievable information. These include computers, digital resources, Interactive Whiteboards, digital cameras and video cameras. ICT is concerned with the handling of electronic information and involves creating, collecting, holding, processing, presenting and communicating this information in a variety of ways for a variety of purposes.

As ICT underpins the effective and efficient delivery of services by any institution, it is therefore important and imperative that Policy is put into place regarding its usage to avoid abuse, misuse or blatant disregard for mission critical data/information. Like any institution which day to day operations are centered around IT as an enabling tool, the need to put into policy that will protect the usage of its ICT resources cannot be overemphasized, hence this document. This document shall apply to all staff and contractors of the Programme Management Unit/Ministry be it located in the main Headquarters of the Ministry on in out posted field offices

Review

Because of the rapidly changing nature of technology this policy will be reviewed on an annual basis by the ICT Team to reflect changes in the ICT infrastructure.

1.1 **Approval**

Authorized users shall request approval from the Office of the Deputy Minister for Administration or the Director of the Programme Management Unit or head of out posted offices or his/her designated ICT Specialist before installing any software that has not been previously approved for use by the PMU/Ministry of Agriculture.

1.2 **Records Treatment**

Authorized users shall not alter, destroy, misplace or render useless any ICT record that is intended to be kept as a record by PMU/MOA in keeping with the applicable PMU/MOA record retention policies.

1.3 **Data Access**

Access to, possession of, or distribution of data shall be in accordance with PMU/MOA regulations, rules, policies and procedures applicable to such data.

1.4 **Limited Personal Use**

1.4.1 Conditions

Authorized users shall be permitted limited personal use of ICT resources, provided that such use:

- Is consistent with the highest standards of conduct for international civil servants and complies with the restrictions expressed in para 5.1 below.
- Is consistent with the interests of the Organization and the maintenance of its reputation.
- Involves minimal additional expense to the PMU/PMU/MOA
- Takes place during personal time or, if during working hours, does not impinge on such working hours
- Is consistent with the ability of the user or other users to perform official functions
- Is consistent with the continuous operation of the PMU/PMU/MOA and the functioning of ICT resources

1.4.2 **Personal Use Rights**

Personal use is a privilege that may be modified or withdrawn at any time, depending on the needs of the PMU/MOA. Authorized users shall bear full responsibility and liability in connection with their personal use of ICT resources and the PMU/MOA shall not bear any responsibility or liability in respect thereof.

When making personal use of ICT resources, authorized users shall ensure that any such use clearly indicates that it is personal and not official in nature.

2.1 Prohibited Activities

2.1.1 **Prohibited Actions**

The ICT Environment must be used in a responsible manner. The use, transmission, distribution, or storage of any material in violation of the PMU/MOA policies and procedures is prohibited. Information sent, received or retrieved through the ICT Environment, including electronic mail, data, documents, programs, images or other forms of communication, may not contain content that may reasonably be considered threatening, harassing, or offensive to any individual, or which is in violation of the PMU/MOA Policy. Such content includes, but is not limited to, sexually explicit or pornographic comments or images, threat of use of force, or any comments that might reasonably be considered offensive in terms, *inter alia*, of race, colour, religious belief, gender, sexual orientation, age, national origin, disability, or political beliefs.

Users of ICT resources and ICT data shall not engage in any use in violation of this standard, including, but not limited to any of the following actions:

- Knowingly, or through gross negligence, creating false or misleading ICT data
- Knowingly, or through gross negligence, making ICT resources or ICT data available to persons who have not been authorized to access them
- Knowingly, or through gross negligence, using ICT resources or ICT data in a manner contrary to the rights and obligations of authorized users
- Knowingly and without justification or authorization, or through gross negligence, damaging, deleting, deteriorating, altering, extending, concealing, or suppressing ICT resources or ICT data, including connecting or loading any non-ICT resources or ICT data onto any ICT resources or ICT data
- Using peer-to-peer file sharing networks in order to illegally obtain copyrighted material, installing software that has not been approved for the PMU/MOA use and hosting internet sites unrelated to the PMU/MOA and its mandate that is not part of a project/programme activity in accordance with the respective programme documents (e.g AWP etc)
- Knowingly accessing, without authorization, ICT data or the whole or any part of an ICT resource, including network transmissions
- Knowingly, or through gross negligence, using ICT resources or ICT data in violation of PMU/MOA contracts or other licensing

agreements for use of such ICT resources or ICT data or in violation of applicable copyright law

- Knowingly, or through gross negligence, attempting, aiding or abetting the commission of any of the activities prohibited by this section
- Using the ICT Environment to create, transmit or store content that may reasonably be considered threatening, harassing, or offensive to any individual, or which is in violation of the PMU/MOA or the Government of Liberia Policy on Workplace Harassment and Abuse of Authority.

3.1 Expectation of Privacy, Personal Information and Confidentiality

3.1.1 Expectation of Privacy

Users are reminded that as a precondition to usage of the ICT Environment, they acknowledge that - and consent to - all data processed by or stored within the ICT Environment is subject to monitoring as explained below.

For the purposes of systems maintenance, diagnostics and performance tuning, ICT Specialists perform technical routine monitoring of systems, including the compilation of aggregated data of systems usage. Automated monitoring is also performed to ensure compliance with this standard and the PMU/MOA Information Security Policy.

PMU/MOA reserves the right, through designated officers, to monitor and review all activities on the IT environment. Information derived from the monitoring of the IT environment may be used to further the course of an official investigation in accordance with relevant PMU/MOA rules and procedures.

3.1.2 Confidentiality

Sensitive data, documents, or information may not be circulated or made available other than for the intended party through any electronic means or otherwise without the prior authorization of the originator of such data, document or information except in the conduct of authorized activities. Any requests for disclosure of sensitive information must be requested from the originator, or if the originator is not known or easily discernable, permission must be requested from the Office of the Minister or the Director of out posted offices. Users should consult the PMU/MOA standard for information sensitivity classification and handling and the PMU/MOA Information Disclosure Policy for proper procedures in information disclosure and handling.

4.1 Rights in ICT Resources; Protection of Technical Integrity and Performance of ICT Resources

4.1.1 Rights to PMU/MOA ICT Resources and Information

- PMU/MOA shall retain all rights in ICT resources and ICT data, including all electronic records and e-mail records, created or received by a Staff member or Non-staff personnel (contractors), subject to the relevant contractual agreement, in connection with or as a result of their official functions. Approved non-PMU/MOA ICT Resources (e.g. personal laptops, smart phones, etc) are also subjects of this provision. By using non-PMU/MOA ICT Resources to create, process, store or disseminate PMU/MOA information or by connecting non-PMU/MOA ICT Resources to the PMU/MOA ICT Infrastructure a user consents to all provisions of this document

- PMU/MOA shall have the right to block or restrict access to any ICT resource or ICT data, at any time and without notice, in accordance with the procedures outlined in paragraph 4.10.1

- Action to block or restrict access may occur when necessary for maintaining or restoring the technical integrity or performance of the system, addressing information security concerns or for any other appropriate purpose, including preventing any of the activities prohibited under section 4.5.1 of this standard. Furthermore, the PMU/MOA retains the right to monitor any traffic traversing its network or any other activity happening on or involving its ICT Systems to ensure use of ICT resources are consistent with this standard as further described below

- Non-PMU/MOA ICT Resources, including laptops may not be connected to the PMU/MOA System (or in any way be used to gain access to PMU/MOA applications) without the explicit approval of the Information Management Associates or ICT Specialist and after verification that such resources meet PMU/MOA's minimum ICT security requirements (such as up-to-date anti-virus software, enabled firewall, no network scanning software or other objectionable software)

5.1 Technical Monitoring

5.1.1 Technical Monitoring and Investigation

All use of ICT resources and ICT data may be subject to technical monitoring and investigation as set forth in Sections 4.9 and 4.10 of this standard. Technical monitoring shall be conducted by the Information Communication technology unit(ICT) of PMU/MOA while investigations shall be conducted by the Office of the Internal Audit in accordance with the Ministry Legal Framework for Addressing Non-Compliance with Standards of Conduct and audit Guidelines. ICT or Internal Audit shall not conduct or assist in any investigation of an individual or individuals, without being requested to do so by authority of the PMU/MOA/PMU.

5.1.2 Monitoring Officials

Officials monitoring or investigating the use of ICT resources shall have access to all ICT Resources and ICT data, including data files, word processing files, e-mail messages, records stored on the local network, Intranet/Internet access records, computer hardware and software, telephone services and any other data accessible to or generated by authorized users provided such access is necessary to complete the technical monitoring or investigative function, as the case may be.

6.1 Technical Monitoring conducted by ICT or Corresponding Offices Away from the PMU/MOA Headquarters

6.1.1 ICT Monitoring

Technical monitoring of the use of ICT resources is routinely performed by the ICT unit/PMU/MOA for troubleshooting, diagnostics, statistical analysis and performance tuning. This may include the compiling of aggregated data for a general monitoring of usage.

6.1.2 Use Reportage

Users should report any incident which affects the confidentiality, integrity or availability of resources and/or information to either their management, ICT Specialist

7.1 Process of Suspending Access

7.1.1 Suspension of Access in Response to External Threats

Misuse or abuse of the ICT Environment by an authorized user, or failure to comply with the requirements of this standard, may constitute a breach of the PMU/MOA Information Security Policy, and result in the suspension, modification or monitoring of access. In order to mitigate risk to the reputation of PMU/MOA, a PMU/MOA user's access to ICT resources may be suspended, modified or monitored at any time. The suspension, modification or monitoring of access to ICT resources for the purpose of risk mitigation requires the approval of the Director of the PMU and the Deputy Minister for Planning and Development of the Ministry of Agriculture. In cases where an Information Security incident* may involve either legal action or an internal investigation, the ICT Specialist may, in consultation with the PMU Director and Legal personnel Office of the PMU/MOA, authorize the collection, tracking and retention of use of ICT resources and its subsequent provision to the legal Advisor of PMU/MOA

In the event a situation requires an immediate response to mitigate the risk of a compromise to the confidentiality, integrity or availability of information resources, the ICT Specialist of the PMU may act immediately and later seek the approvals of PMU Director, the

PMU/MOA Legal Office, within 48 hours. The access rights may be then be re-established should the risks be mitigated and following consultation between the persons authorizing the suspension.

*An information security incident is any action either intentional or unintentional which adversely affects the confidentiality, integrity or availability of PMU/MOA information.

8.1 Inputs

Structure Element - Inputs

8.1.1 **Definitions**

a. ICT environment: The computing and data processing systems that include, but are not limited to, the local area networks, the wide area networks, workstations, laptops, fixed or removable storage media, messaging systems, Internet access, voice mail, facsimile, telephone access, SMS, and related technologies.

b. Authorized user: PMU/MOA Staff members and all other persons who are appropriately authorized to access and use the PMU/MOA's ICT Environment, including those persons with remote access to the ICT environment.

c. Authorized software and equipment: Software and equipment for which a user has received the required authorization for access or use from the Ministry authority or its out posted offices head Directors, the Project Coordinator or the ICT Specialist. In cases in which users have received the required authorization for remote access, the user is provided by PMU/MOA with the authorized software and equipment for this purpose.

d. Personal Use: The utilization of resources of the ICT environment for purposes other than those directly associated with a users' contract, employment or function at PMU/MOA.

Structure Element - Deliverables

9.1 Roles and Responsibilities

Structure Element - Roles & Responsibilities

9.2 Conditions Applicable to Use of ICT Resources and ICT Data. The following conditions apply to the use of ICT resources and data within PMU/MOA:

9.3. **Obligations**

Authorized users shall ensure that their use of ICT resources and ICT data is consistent with their obligations as Staff members or with such other contractual or related obligations as may apply to them as Non-staff personnel, as the case may be.

9.4 **Accuracy and Protection**

Authorized users shall use their best efforts to:

- Ensure the accuracy of any ICT data for which they are responsible
- Preserve and protect ICT resources and ICT data which may be needed by the PMU/MOA for any purpose

10.1 **Additional Info. and Tools**

Structure Element - Additional Info & Tools
Annex A – Principles for Allocation and Termination of Access Credentials to PMU/MOA ICT Systems and Resources

10.2. The issuance of access credentials to PMU/MOA ICT systems and resources (including the email system) must be justified by an identified PMU/MOA business need and a need-to-know on the part of the requesting party which shall have contractual relationship with PMU/MOA.

10.3 It should be recognized that issuing access credentials (including email accounts) to personnel without a contractual relationship with PMU/MOA raises potential risks to PMU/MOA and therefore the burden of proof rests with the non-PMU/MOA entity to justify why access to PMU/MOA ICT systems and resources (including email system) advances the business needs of PMU/MOA.

10.4 By using credentials to access and/or use PMU/MOA ICT systems and resources, non-PMU/MOA entity acknowledges that they shall be subject of relevant PMU/MOA ICT policies, standards and procedures and shall not share IT information to entities outside of PMU/MOA without the express consent of the PMU Director. Any exceptions to this policy must be approved by the PMU/MOA Director.

PMU/MOA Access Credentials

11.1 Access credentials to PMU/MOA ICT systems and resources (including email accounts) will be assigned to a specific person and used only by that person. Issuance of access credentials and email accounts to persons who do not have a contractual relationship with PMU/MOA shall be done only if there is a compelling PMU/MOA business need to do so and must have the written approval of the ICT Specialist acting on behalf of the PMU Director or Project Coordinator.

12.1 ICT Specialist and IT Assistant will issue email accounts on behalf of their users. Within PMU/MOA, there is one type of email account, .**@moa.gov.lr** which uses the naming convention of **initial+lastname@moa.gov.lr**.

Account and Access Maintenance

13.1 Access to PMU/MOA ICT Systems and resources are to be considered a privilege and not an entitlement. Access credentials are granted specifically for the purpose of performing PMU/MOA's business. As such, these credentials shall be maintained at a minimum as long as the person to whom the account is assigned continues to conduct PMU/MOA business.

14.1 Accounts will be implemented only as stated below and will apply to all PMU/MOA managed accounts. For PMU/MOA Staff members, the following applies:

a. When a Staff member is on administrative leave, his/her access credentials (including email account) may be suspended unless a decision is made by the Project Coordinator (in consultation with PMU Director and ICT Specialist) to keep them active.

b. When a Staff member is on inter-project or inter-ministry movement (e.g. secondment, loan exchange) to another ministry, his/her access credentials (including email account) will remain active for the duration of the Staff member's appointment with PMU/MOA.

c. When a Staff member is separating from the PMU/MOA, his/her access credentials to PMU/MOA ICT Systems and resources (including email account) will be suspended as of the date of separation (i.e. the user cannot access or use the account to send emails) and deleted 60 days thereafter. Access credentials may, however, be extended by the employee's supervisor or their designated representative for up to 90 days. This proposed change eliminates the need to get PMU Director's approval for any email extension.

If needed, the account may have automatic forwarding enabled to another email account provided that the user cannot access their old PMU/MOAliberia.org account. The forwarding shall be discontinued when the account is deleted.

d. When a Staff member is subject to dismissal or separation for disciplinary actions, his/her access credentials to PMU/MOA ICT Systems and resources (including email account) will be suspended on the date of separation and deleted 60 days thereafter.

e. When Staff member is retiring from PMU/MOA, their access credentials (including **moa.gov.lr** email account) will be suspended as of the date of retirement and deleted 60 days thereafter.

f. On an exceptional basis, a suspended account may be re-activated. The request should be made in writing to the PMU Director from the Project Coordinator specifying the reason for needing to re-activate the account and a specific time period for which the account will remain active. The request should not come directly from the person requesting the extension. The PMU Director will make the final decision on the re-activation of suspended accounts.

g. Any type of access credentials to PMU/MOA ICT Systems and resources (including email accounts) given to non-PMU/MOA staff shall only be granted to the date of contract termination up to a maximum period of 1 year. The non-PMU/MOA entity must re-justify/confirm the continued need for access credentials. In the absence of a justification to continue, access credentials (including email account) shall be terminated or suspended at the contract termination date or 1 year from the date of account creation, whichever is sooner.

h. For those individuals who may pose a risk to the reputation, ICT Systems or resources of PMU/MOA, the suspension of corresponding access credentials requires the approval of the Director of PMU and Project Coordinator.

15.1 Access credentials to the PMU/MOA ICT Systems and resources (including email accounts) given to PMU/MOA staff shall be suspended or deleted if no activity has been recorded for such credentials for 180 days.

16.1 For non-PMU/MOA organizations having an MOU with the PMU/MOA, those organizations are responsible for provisioning, maintaining and de-provisioning their own user accounts. Access to the PMU/MOA ICT Systems and resources shall be granted by the PMU/MOA in accordance with the terms of the MOU.

17.1 It is the responsibility of the office/department/unit to which the PMU/MOA staff member or non-staff personnel belongs to coordinate with the appropriate procurement offices as applicable, to ensure that the necessary access credentials actions are promptly taken. The expiry date on any accounts created for PMU/MOA personnel or contractors shall be their contract expiration date. Any request for an exceptional extension of access, for compelling business reasons, beyond the contract expiration date should follow the provisions outlined in para 8 f above.

.

Annex B – Individual Backups

Individual backup procedures are as follows:

- All authorized users are required to perform regular backups and store backup information in a secure yet accessible manner so that they can perform their functions appropriately utilizing procedures available in their local offices or in consultation with their unit's/department's responsible IT management

- All authorized users are responsible for keeping copies of official information and data on shared drives. These backups should also include any emails that are stored locally (POP) rather than on the PMU/MOA system (IMAP).

- ICT Specialist and IT Assistant of the PMU/MOA are responsible for backing up shared drives and keeping backup media in secure and accessible off-site locations

- All authorized users should consult with the ICT Specialists and IT Assistant to establish procedures for the regular backup of their files

ANNEX C – Passwords

1. Password Complexity

1.1 All passwords (either manually or automatically generated) for all types of credentials should satisfy the following complexity requirements.

1.2 The password must:

- Contain eight characters or more
- Contain characters from three of the following four character classes:

a. English uppercase characters (i.e. a-z)
b. English lowercase characters (i.e. A-Z)
c. Base 10 digits (i.e. 0-9)
d. Punctuation and other characters (i.e. !@#$%^&*()_+|~-=\` {}[]:";'<>?,./)

1.3 The password must not be:

- A derivative of the user name
- A derivative of user related information (e.g. name, telephone number, birthday, etc.)
- A consecutive and/or identical, numeric or alphabetic pattern (e.g. abcdef, qwerty, 11111, etc.)

2. Password management system

2.1 Any system that provides ability for a user to log-on (including administrative access to servers and network equipment), change or reset a password shall:

- Enforce the use of individual user IDs and passwords to maintain accountability

- Enforce a choice of quality passwords in accordance with password complexity requirements
- Enforce password change every ninety (90) days
- Require an old password in order to change it.
- Force users to change temporary passwords at the first log-on
- Maintain a record of four (4) previous user passwords and prevent re-use of them
- Not display passwords on the screen when being entered
- Store password files separately from application system data
- Store and transmit passwords in protected (encrypted or hashed) form

3.1 Where possible, users should be given a warning that their password is going to expire at least five (5) days but not more than ten (10) days prior to expiration.

3.2 Passwords shall not be sent in unencrypted form over the network (e-mail message, IMAP login, etc.).

3.3 ICT personnel shall not reset user's password unless a user first definitively identifies him or herself and the change shall only be done with written request. No password changes should be effected based on verbal request. Request could be in sms text format, email request etc.

4. User Responsibilities

4.1 Users shall keep his/her credentials confidential. User must not knowingly or through gross negligence share a password with anyone, including members of their family, their manager, co-workers or ICT personnel.

4.2 Users should not use the same password for PMU/MOA (e.g. **@moa.gov.lr** email account, Intranet, etc.) and non-PMU/MOA access credentials (e.g. personal email account).

4.3 Users should not use the "Remember Password" feature in a web browser or web application as the security of the password/cookie storage may be compromised.

4.4 User shall avoid keeping a record (e.g. paper, software file or hand-held device) of passwords, unless this can be stored securely and the method of storing has been approved by the ICT Specialist of the PMU.

4.5 Users shall change temporary passwords at the first log-on.

4.6 User shall change passwords whenever there is any indication of possible system or password compromise.

5. Secure log-on procedures

5. When applicable, access to a system should be controlled by a secure log-on procedure. The log-on procedure should disclose the minimum of information in order to minimize the opportunity for unauthorized access.

5.1 A good log-on procedure should:

- Not display system or application identifiers until the log-on process has been successfully completed
- Display a general notice warning that the computer should only be accessed by authorized users (reference to the old log-on banner standard)
- Not provide help messages during the log-on procedure that would aid an unauthorized user
- Validate the log-on information only on completion of all input data. If an error condition arises, the system should not indicate which part of the data is correct or incorrect
- Limit the number of unsuccessful log-on attempts allowed to three (3) attempts
- Force a time delay between each of the three log-on attempts
- Temporary prevent further log-on attempts for the period of five (5) minutes when limit is reached
- Record unsuccessful and successful attempts
- Record (log) an alarm message if the maximum number of log-on attempts is reached and account is suspended
- Display the following information on completion of a successful log-on:
    - date and time of the previous successful log-on
    - details of any unsuccessful log-on attempts since the last successful log-on
    - Not display the password being entered or consider hiding the password characters by symbols
    - Not transmit passwords in clear text over a network.

Acronym

MOA	Ministry of Agriculture
ICT	Information Communications Technology
POP	Post Office Protocol
IMAP	Internet Messaging Access Protocol
PMU	Programme Management Unit
MOU	Memorandum of Understanding

Approved by: _____

Director/Programme Management Unit/MOA

Date: _____