Information Technology

Standard and Guidelines

Version 1.0

EOTC - DICAC

Refuge & Returnee Affairs Department

This Standard and Guidelines will be reviewed, and revised as necessary, by ICT Unit , annually or more frequently as circumstances require.

EOC-DICAC /RRAD

Street: Queen Elisabeth II

PO Box: 31247

Addis Ababa, Ethiopia

Telephone: 011-1-552221

Table of Contents

1. About the Information Technology Standard and Guidelines

RRAD provides and maintains technological products, services and facilities like Personal Computers (PCs), peripheral equipment, servers, telephones, Internet and application software to its employees for official use. The Information Technology (IT) Standard and Guidelines of the RRAD defines rules, regulations and guidelines for proper usage and maintenance of these technological assets to ensure their ethical and acceptable use and assure health, safety and security of data, products, facilities as well as the people using them. It also provides guidelines for issues like purchase, compliance, IT support and employees pertaining to technological assets and services used for office work.

Published Date **: 01-06-2021**
Next Review Date **: 31-12-20**22

1.1. Purchase

1.1.1. The Procurement is responsible to purchase new technological equipment, services or software for official purposes as per the approval of IT unit.

1.1.2. All approved equipment, services or software will be purchased through the Procurement Unit , unless informed/permitted otherwise.

1.1.3. IT Unit will assist the Procurement Unit while evaluating potential supplier best and most cost-effective hardware or software to be purchased for a particular unit/project/purpose based on the requirement.

1.2. Compliance

1.2.1. All employees & units are expected to comply with the IT Standard and Guidelines rules while requesting, purchasing, and using and maintaining any equipment or software purchased or provided by the Firm.

1.2.2. Any employee who notices misuse or improper use of equipment or software within the firm must inform to IT Unit immediately.

1.2.3. Inappropriate use of equipment and software by an employee will be subject to disciplinary action as deemed fit by the Management Committee of RRAD.

1.3. Employee Training

1.3.1. Basic IT training and guidance is provided to all new employees about using and maintaining their Personal Computer (PC), peripheral devices and equipment in the RRAD, accessing the RRAD network and using application software.

1.3.2. Employees can request and/or the Management and IT Unit can decide to conduct an IT training on requirement basis.

1.4. IT Support

1.4.1. RRAD uses a telephone & remote system to provide IT Support to its employees and clients in addition to physical checkup.

1.4.2. Employees may need hardware/software installations or may face technological issues this cannot be resolved on their own. Employees are expected to get help from the IT Unit for such issues via Email or Telephone system.

1.4.3. For the sake of quick understanding, employees are expected to provide details of their issue or help required in Support Email sent.

1.4.4. For major issues like PC replacement, non-working equipment, and installation of application software and more, it is mandatory for all employees to inform the IT Unit immediately.

1.4.5. For any damage to Personal Computers, approval from line Manager would be required for parts/PC replacements.

2. Equipment Usage Standard and Guidelines

2.1. Objective

The Equipment Usage Standard and Guidelines informs employees and managers about equipment purchase, Office-Level and project-level inventory management, rules for allocating & transferring equipment to employees, departments or projects and best practices for all equipment usage and maintenance.

2.2 Equipment Purchase

2.2.1. The following equipment is purchased by the RRAD and provided to individual Employees, departments or projects for RRAD official use. The list can be modified when required.

A. Personal Computing Devices (Desktop, Laptop, Tablet)
B. Computer Peripherals (Printer, Scanner, Photocopier, Fax Machine, Keyboard, Mouse, Web Camera, Speaker, etc.)
C. Networking Equipment & Supplies (Router, Switch, WIFI, Wiring, etc.)
D. Cell phones

2.2.2. The Procurement unit will maintain a small inventory of standard PCs, software and equipment required frequently to minimize delay in fulfilling critical orders and IT unit assist in preparing updated standard list of IT resources..

2.3. Inventory Management

2.3.1. The Procurement and store Units are responsible for maintaining an accurate inventory of all technological assets, software and tangible equipment purchased by the RRAD.

2.3.2. The following information is to be maintained for above mentioned assets in an Inventory Sheet:

A. Item
B. Brand/ Company Name
C. Serial Number
D. Basic Configuration (e.g. HP Laptop, 120 GB HD, 2 GB RAM etc.)
E. Physical Location
F. Date of Purchase
G. Purchase Cost
H. Current Person In-Charge

2.3.3. Proper information about all technological assets provided to a specific dep't, project or unit must be regularly maintained in their respective Inventory Sheets by an assigned coordinator from that dept., division , project or unit on a regular basis. The information thus maintained must be shared with the IT, store and Procurement Unit as and when requested.

2.3.4. When an Inventory Sheet is updated or modified, the previous version of the document should be retained. The date of modification should be mentioned in the sheet.

2.3.5. All technological assets of the RRAD must be physically tagged with codes for easy Identification by warehouse unit with the assistance of IT section.

2.3.6. Periodic inventory audits will be carried out by the store Unit to validate the inventory and make sure all assets are up-to-date and in proper working condition as required for maximum efficiency and productivity.

2.4. Equipment Allocation, De-allocation & Relocation

2.4.1. **Allocation of Assets:**

A. New Employees may be allocated a personal computer (desktop or laptop) for office work on the Day of Joining, only and only as per work requirement.
B. If required, employees can request their unit line Manager(s) for additional equipment or supplies but with the approval of IT unit and Dept. manager.

2.4.2. **De-allocation of Assets:**

A. It is the line Manager's and IT Unit responsibility to collect all allocated RRAD equipment & other assets from an employee who is leaving RRAD.
B. Updating the Inventory Sheet is mandatory after receiving back all allocated equipment to store unit.
C. The received assets must be returned back to the Store/ Warehouse Unit

2.5 Equipment Usage, Maintenance and Security

2.5.1. It is the responsibility of all employees to ensure careful, safe and judicious use of the equipment & other assets allocated to and/or being used by them.

2.5.2. Any user will be expected to have only one desktop or one Laptop as per the work require, which might be desktop or laptop, a user may have one standalone printer or shared printer as per the work needed. However if the work demands two computer, it might be seen in management to allocate both for a user but not recommended.

2.5.3. Any observed malfunction, error, fault or problem while operating any equipment owned by the RRAD or assigned to you must be immediately informed to the IT Unit. Any repeated occurrences of improper or careless use, wastage of supplies or any such offense compromising the safety or health of the equipment and people using them will be subject to disciplinary action.

2.5.4. If your assigned computing device is malfunctioning or underperforming and needs to be replaced or repaired, then written approval from your line Manager is required for the same. The malfunctioning device needs to be submitted to the IT Unit for checking, Maintenance or repair. The IT Unit staff person will give a time estimate for Repair/maintenance or other decision.

2.5.5. RRAD uses CCTV security camera system for security purposes to public areas only and recorded video will be also stored on storage media which is accessed only by authorized personnel and the IT unit & management of RRAD will oversight temporarily or permanently the surveillance video camera.

2.6 Phone Usage Standard and Guidelines

2.6.1. Landline phone systems are installed in the RRAD's offices to communicate internally with other employees and make external calls.

2.6.2. The landline phones should be strictly used to conduct official work only. As far as possible, no personal calls should be made using landline phones owned by the RRAD.

2.6.3. Long distance calls should be made after careful consideration since they incur significant costs to the RRAD.

2.6.4. The General Service and IT Unit is responsible for maintaining telephone connections in offices. For any problems related to telephones, they should be contacted.

2.6.5. Employees should remember to follow telephone etiquette and be courteous while representing themselves and the RRAD using the RRAD's phone services.

3. Personal Computer (PC) Standards

3.1. Objective

The main aim of this Standard and Guidelines is to maintain standard configurations of PC hardware and software
purchased by the RRAD and provided to employees for official work. The hardware standards will help maintain optimum work productivity, computer health & security and provide timely and effective support in troubleshooting PC problems. The software standards will ensure better system administration, effective tracking of software licenses and efficient technical support.

3.2. General Guidelines

3.2.1. It is the responsibility of the IT Unit to establish and maintain standard configurations of hardware and software for PCs owned by the RRAD. The standard, can however, be modified at any point in time as required by the IT Unit in consultation with the Management .

3.2.2. Multiple configurations of standards are maintained as per the different requirements of various Units and projects in the RRAD, in consultation with the Dept./Project Head and IT unit.

3.3.3. Only in exceptional cases, when none of the standard configurations satisfy the work requirements, can an employee request a non-standard PC configuration. Valid reasons need to be provided for the request and written approval of the line
required for the same.

3.3. Network Access

3.3.1. All PCs being used in the RRAD are enabled to connect to the RRAD's Local Area Network as well as the Internet.

3.3.2. Network security is enabled in all PCs through Firewall, Web Security and Kaspersky Security software.

3.3.3. Employees are expected to undertake appropriate security measures as enlisted in the IT Standard and Guidelines.

3.4. Data Backup Procedure

3.4.1. Data Backup is setup during installation of Operating System in a PC. As an additional security measure, it is advised that employees keep important official data in some external storage device also.

3.4.2. File Backup System

A. RRAD will be installing file storage on server for backing up data of all employees. All employees are expected to keep official data on the file system.

B. All employees will login to the file storage server through RRAD user ID and password.

3.5. Antivirus Software

3.5.1. Approved licensed antivirus software is installed on all PCs owned by the RRAD.

3.5.2. Two configurations – Basic and Advanced are maintained for Antivirus software installed on RRAD's computers. The configurations are installed on PCs as per work requirement of particular unit/Project./employee.

3.5.3. Employees are expected to make sure their Antivirus is updated regularly. The IT Unit should be informed if the Antivirus expires.

3.5.4. Any external storage device like pen drive or hard disk connected to the PC needs to be completely scanned by the Antivirus software before opening it and copying files to/from the device.

3.5.5. Personal laptops which are connected to RRAD network, should have expected to have Antivirus otherwise shouldn't connect to RRAD net.

3.6 PC Support

3.6.1. Guidance and tips given by the IT Unit for designated staff for maintaining the PC should be remembered while using a PC.

3.6.2. The IT Unit should be contacted via IT Support Email or telephone any assistance with your PC hardware or software.

3.6.3. Technical support will not be provided for hardware devices or software which is personally purchased, illegal or not included in the standard hardware/software list developed by the IT Unit.

3.6.4. Software applications evaluated by the IT Unit to cause problems with the RRAD's PCs will be removed.

3.6.5. Any user cannot install any software on RRAD computers or devices without the permission or knowledge of the IT unit.

4. Internet Usage Standard and Guidelines

4.1. Objective

The Internet Usage Standard and Guidelines provides guidelines for acceptable use of the RRAD's Internet network so as to devote Internet usage to enhance work productivity and efficiency and ensure safety and security of the Internet network, RRAD data and the employees.

4.2. General Guidelines

4.2.1. Internet is a paid resource and therefore shall be used only for office work.

4.2.2. The RRAD reserves the right to monitor, examine, block or delete any/all incoming or outgoing internet connections on the RRAD's network.

4.2.3. RRAD has systems in place to monitor and record all Internet usage on the RRAD's network including each website visit, and each email sent or received. The IT unit and the Management can choose to analyze Internet usage and publicize the data at any time to assure Internet usage is as per the IT Standard and Guidelines.

4.2.4. RRAD has installed an Internet Firewall to assure safety and security of the RRAD network. Any employee who attempts to disable, RRAD or circumvent the Firewall will be subject to strict disciplinary action.

4.3. Internet Login Guidelines

4.3.1. Username and password for a new employee must be requested by the line Manager.

4.3.2. Sharing the Username and Password with another employee, visitor or guest user is prohibited.

4.3.3. A visitor or guest user who wants to use the office Internet will be given a Guest Username and Password by IT unit.

4.3.4. The IT Unit will define guidelines for issuing new passwords or allowing employees to modify their own passwords.

4.3.5. Any password security breach must be notified to the IT Unit immediately.

4.3.6. Username and password allotted to an employee will be deleted upon Resignation/termination/retirement from the RRAD.

4.4. Password Guidelines

The following password guidelines can be followed to ensure maximum password safety.

4.4.1. Select a Good Password:

A. Choose a password which does not contain easily identifiable words (e.g. your username, name, phone number, house location etc.).
B. Use 8 or more characters.
C. Use at least one numeric and one special character apart from letters.
D. Combine multiple unrelated words to make a password.

4.4.2. Keep your Password Safe

A. Do not share your password with anyone.
B. Make sure no one is observing you while you enter your password.
C. As far as possible, do not write down your password. If you want to write it down, do no display it in a publicly visible area.
D. Change your password periodically (every 3 months is recommended).
E. Do not reuse old passwords.

4.4.3. Other Security Measures

A. Ensure your computer is reasonably secure in your absence.

4.5. Online Content Usage Guidelines

4.5.1. Employees are solely responsible for the content accessed and downloaded using Internet facility in the office. If they accidentally connect to a website containing material prohibited by the RRAD, they should disconnect from that site immediately.

4.5.2. During office hours, employees are expected to spend limited time to access news, social media and other websites online, unless explicitly required for office work.

4.5.3. Employees are not allowed to use Internet for non-official purposes using the Internet facility in office.

4.5.4. Employees should schedule bandwidth-intensive tasks like large file transfers, video downloads, mass e-mailing etc. for off-peak times.

4.7. Inappropriate Use

The following activities are prohibited on RRAD's Internet network. This list can be modified/updated anytime by the Management Committee as deemed fit.

Any disciplinary action considered appropriate by the Management Committee (including legal action or termination) can be taken against an employee involved in the activities mentioned below on RRAD devices .

4.7.1. Playing online games, downloading and/or watching games, videos or entertainment software or engaging in any online activity which compromises the network speed and consumes unnecessary Internet bandwidth.

4.7.2. Downloading images, videos and documents unless required to official work.

4.7.3. Accessing, displaying, uploading, downloading, storing, recording or distributing any kind of pornographic or sexually explicit material unless explicitly required for office work.

4.7.4. Accessing pirated software, tools or data using the official network or systems.

4.7.5. Uploading or distributing software, documents or any other materials (sexually explicit, racist, discriminatory, illegal or unlawful, offensive or obscene materials) owned by the RRAD online without the explicit permission of the Management Committee.

4.7.6. Engaging in any criminal or illegal activity or violating law.

4.7.7. Invading privacy of coworkers and use of another employee's computer or email to carry out any of activities prohibited above.

4.7.8. Using the Internet for personal financial gain or for conducting personal business or access without the permission (hacking) any computer.

4.7.9. Deliberately engaging in an online activity which hampers the safety & security of the data, equipment and people involved.

4.7.10. Carrying out any objectionable, frivolous or illegal activity on the Internet that shall damage the RRAD's reputation.

4.7.11. Connect internet (cable or Wi-Fi) to personal services (such as personal email services or others) during working hours using RRAD or personal equipment's.

5. Information Security Standard and Guidelines

5.1. Objective

Information security means protection of the RRAD's data, applications, networks and computer systems from unauthorized access, alteration and destruction. The Information Security Standard and Guidelines provides guidelines to protect data integrity based on data classification and secure the RRAD's information systems.

5.2. General Guidelines

5.2.1. Various methods like access control, authentication, monitoring and review will be used to ensure data security in the RRAD.

5.2.2. Security reviews of servers, firewalls, routers and monitoring systems must be conducted on a regular basis. These reviews should include monitoring of access logs and intrusion detection software logs.

5.3. Data Classification

5.3.1. The RRAD classifies data into three categories:

A. High Risk

It includes information assets which have legal requirements for disclosure and financial penalties imposed for disclosure.

E.g. Payroll, personnel, financial, biometric data

B. Medium Risk

It includes confidential data which would not impose losses on the RRAD if disclosed, but is also not publicly available.

E.g. Agreement documents, unpublished reports, etc.

C. Low Risk

It includes information that can be freely disseminated.

E.g. brochures, published reports, other printed material etc.

5.3.2. Different protection strategies must be developed by the IT Unit for the above three data categories. Information about the same must be disseminated appropriately to all relevant staffs.

5.3.3. High risk data is secured properly.

5.3.4. All data must be backed up on a regular basis as per the rules defined by the IT Unit at that time.

5.4. Access Control

5.4.1. Access to the network, servers and systems in the RRAD will be achieved by logins and will require authentication. Authentication includes the use of passwords.

5.4.2. All users of systems which contain high or medium risk data must have a strong password as defined in the IT Standard and Guidelines.

5.4.3. Default passwords on all systems must be changed after Domain login.

5.5. Virus Prevention

5.5.1. Virus prevention for personal computers, Mobile and email usage has been described previously. All RRAD laptops and desktop computers are fully should installed Licensed Kaspersky Antivirus.

5.5.2. Apart from that, all servers and workstations that connect to the network must be protected with licensed anti-virus. The software must be kept up-to-date.

5.5.3. Whenever feasible, IT unit must inform users when a virus/ other vulnerability has been detected in the network or systems or removed the device from network and repeated action of this may a user blocked from RRAD network.

6. Email & Chat Standard and Guidelines

6.1. Objective

This Standard and Guidelines provides information about acceptable usage, ownership, confidentiality and security while using electronic messaging systems and chat platforms provided or approved by the RRAD. The Standard and Guidelines applies to all electronic messages sent or received via the above mentioned messaging systems and chat platforms by all official employees of the RRAD.

6.2. General Guidelines

6.1. RRAD reserves the right to approve or disapprove which electronic messaging systems and chat platforms would be used for official purposes. It is strictly advised to use the pre-approved messaging systems and platforms for office use only.

6.2. An employee who, upon joining the RRAD, is provided with an official email address should use it for official purposes only.

6.3. Any email security breach must be notified to the IT Unit immediately.

6.4. Upon termination, resignation or retirement from the RRAD will deny all access to electronic messaging platforms owned/provided by the RRAD.

6.5. Electronic mails and messages should be sent after careful consideration since them are inadequate in conveying the mood and context of the situation or sender and might be interpreted wrongly.

6.6. All email signatures must have appropriate designations of employees.

6.3. Ownership

6.3.1. The official electronic messaging system used by the RRAD is the property of the RRAD and not the employee. All emails, chats and electronic messages stored, composed, sent and received by any employee or non-employee in the official electronic messaging systems are the property of the RRAD.

6.3.2. IT Administrator can change the email system password and monitor email usage of any employee for security purposes.

6.4. Confidentiality

6.4.1. Proprietary, confidential and sensitive information about the firm or its employees should not be exchanged via electronic messaging systems unless pre-approved by the Management .

6.4.2. Caution and proper judgment should be used to decide whether to deliver a message in person, on phone or via email/electronic messaging systems.

6.4.3. Before composing or sending any message, it should be noted that electronic messages can be used as evidence in a court of law.

6.4.3. Unauthorized copying and distributing of copyrighted content of the RRAD is Prohibited.

6.5. Email Security

6.5.1. **Anti-Virus**

A. Anti-virus software pre-approved by the IT Unit should be installed in the laptop/desktop provided to a new employee after joining the RRAD.

B. All employees in the RRAD are expected to make sure they have anti-virus software installed in their laptops/desktops (personal or official) used for office work, Otherwise couldn't join the RRAD network

C. RRAD will bear responsibility for providing, installing, updating and maintaining records for one anti-virus per employee at a time for the official laptop/Desktop provided by the RRAD. The employee is responsible for installing good quality anti-virus software in their personal laptop/desktop used for office work.

D. Employees are prohibited from disabling the anti-virus software on RRAD-provided laptops/desktops.

E. Employees should make sure their anti-virus is regularly updated and not out of date.

6.5.2. Safe Email Usage: Following precautions must be taken to maintain email security:

A. Do not to open emails and/or attachments from unknown or suspicious sources unless anticipated by you.

B. In case of doubts about emails/ attachments from known senders, confirm from them about the legitimacy of the email/attachment.

C. Use Email spam filters to filter out spam emails.

6.6. Inappropriate Use

6.6.1. Official Email platforms or electronic messaging systems including but not limited to chat platforms and instant messaging systems should not be used to send messages containing pornographic, defamatory, derogatory, sexual, racist, harassing or offensive material.

6.6.2. Official Email platforms or electronic messaging systems should not be used for personal work, personal gain or the promotion or publication of one's religious, social or political views.

6.6.3. Spam/ bulk/junk messages should not be forwarded or sent to anyone from the official email ID unless for an officially approved purpose.

7. Software Usage Standard and Guidelines

7.1. Objective

The Software Usage Standard and Guidelines is RRAD to provide guidelines for appropriate installation, usage and maintenance of software products installed in RRAD-owned computers.

7.2. General Guidelines

7.2.1. Third-party software (free as well as purchased) required for day-to-day work will be pre-installed onto all company systems before handing them over to employees. A designated person in the IT Unit can be contacted to add to/delete from the list of pre-installed software on RRAD computers. No other third-party software – free or licensed can be installed onto a computer system owned or provided to an employee by the RRAD, without prior approval of the IT Unit.

7.2.2. To request installation of software onto a personal computing device using RRAD Internet /Network system, an employee needs to send a written request via the IT Support Email.

7.3 Compliance

7.3.1. No employee is allowed to install any software on official computing systems without prior to notice to IT unit

7.3.2. Software purchased by the RRAD or installed on RRAD computer systems must be used within the terms of its license agreement.

7.3.3. Any duplication, illegal reproduction or unauthorized creation, use and distribution of licensed software within or outside the RRAD is strictly prohibited. Any such act will be subject to strict disciplinary action.

7.3.4. Any employee who notices misuse or improper use of software within the RRAD must inform IT Unit.

7.4. Software Registration

7.4.1. Software licensed or purchased by the RRAD must be registered in the name of the RRAD with the Job Role or Unit, in which it will be used and not in the name of an individual.

7.4.2. After proper registration, the software may be installed as per the Software Usage Standard and Guidelines of the RRAD. A copy of all license agreements must be maintained by the IT Unit

7.4.3. After installation, all original installation media (CDs, DVDs, etc.) must be safely stored in a designated location by the IT Unit

7.5. Software Audit

7.5.1. The IT Unit will conduct periodic audit of software installed in all RRAD owned systems (computers, cellular devices and on others) to make sure all compliances are being met.

7.5.2. Prior notice may or may not be provided by the IT Unit before conducting the Software Audit.

7.5.3. During this audit, the IT Unit will also make sure the anti-virus is updated, the system is Scanned and cleaned and the computer is free of garbage data, viruses, worms or other harmful programmatic codes and is checking the device is working for the intended purpose.

7.5.4. The full cooperation of all employees is required during such audits.

8. Data Communication

8.1. Objective

Data is vital assets to RRAD and its partners where information will relate to communicational, business research, administrational and management. RRAD is committed to protecting information resources that are critical to its communication, administrative and research mission. These information assets is protected by controlling authorized access, creating logical and physical barriers to u unauthorized access for data communication.

This will ensure that the communication is appropriately secured against the adverse effects of breach in confidentiality, integrity, availability and compliance which would otherwise occur.

8.2. Communication standard

8.2.1. Data is a resource (hard copy /soft copy) so RRAD kept these data's securely and safely.

8.2.2. All information is available to only authorized users.

8.2.3. RRAD classified data's according to an appropriate level of sensitivity value.

8.2.4. Communication of information in RRAD strongly expected to be accurate, complete, timely and consistent.

8.2.5. Users who have access information have responsibility to handle it appropriately according to its classification.

8.2.6. All Information in RRAD is fully protected and restricted against unauthorized access.

8.2.7. Communication of Data at RRAD is strongly expected to be target audiences (donors, the public, governments) and should be focused on messages including the firm Mission.

8.3. Processing Personal Data

Personal data covers any information relating to identifiable natural person including both facts and opinions. It includes name and address, detail of payment of salary, detail of medical recording of an employee/refugee, and so on.

8.3.1. Any information which falls under definition of personal data is not otherwise exempt will remain confidential and will only be disclosed to third parties with the consent of the person.

8.3.2. Any member of RRAD or partners in a way of working in collecting personal data must do in link with the following principles lawfulness, fairness and transparency, Purpose limitation and Data minimization, Accuracy, Storage limitation, Integrity and confidentiality (security) and Accountability.

8.3.3. Any authorized user of RRAD is required to identify data processing and protection in use that is likely to result in a high risk to individuals..

8.3.4. Sensitive information should not be stored anywhere instead in proper ways (in hardcopy and softcopy) and Sensitive personal data of (employee/refugee) should be kept securely and require written request to access it

8.3.5. Subject to the provision of the law, an employee found to have violated this may be subject to disciplinary action, up to and including termination of employment.

The document is found in "PUBLIC "shared folder of your computer in soft copy and at staff Unit head in hard copy by both (English and Amharic format)

Prepared By:

Ato Tewodros Getachew

IT Officer

Refugee & Returnee Affair Department _____

Approved: By

EOTC_DICAC D/ Commissioner
Ato Yilekal Shiferaw _____

EOTC-DICAC- RRAD- D/Manager
Ato Belay Negesse _____

Date: June 16, 2021

Acknowledgment of RRAD IT Standard and Guidelines Form

Please complete this form and return to IT Unit (to be kept on personal file of Admin for Audit purposes)

By signing below, I agree to the following terms

A. I have read a copy of IT Standard and Guidelines f RRAD and confirm my understanding of the content;
B. I agree to comply ,to the best of my ability, with IT Standard and Guidelines
C. I understand and agree that any computers, software and storage media and others telecommunications/IT equipment provided to me by RRAD contains proprietary and confidential information about RRAD and its partners (including donors),suppliers, etc., and that this is and remains the property of RRAD at all times.
D. I agree that I shall not copy ,duplicate (except for backup purposes as part of my job duties here at RRAD),otherwise disclose, or allow anyone else to copy or duplicate any of this information or software;
E. I agree that ,if I leave RRAD any reason, I shall immediately return to the RRAD the original and copy of any and all electronic data, software, computer (desktop and laptop),computer materials, IT equipment's that I have received from the RRAD warehouse unit that is either in my possession or otherwise directly or indirectly under my control.
F. I have read and understand RRAD internet access rule statements in IT Standard and Guidelines and agree to use the internet access granted to me in the pursuit of legitimate RRAD business only. I shall also take all reasonable precautions to ensure my internet access facilities are not available to or used by any other person .Further, I accept that each internet access I make, using RRAD IT equipment may be monitored and audited as part of RRAD measure to ensure IT Standard and Guidelines is maintained.

Name of User:	Job Title:
Date:	Location of Office Base:
Signature:	