ICT Policy
Bangladesh Red Crescent Society (BDRCS)

Table of Contents
1. Introduction ........................................................................................................................................3
2. Objective ........................................................................................................................................3
3. Applicability & Scope ..................................................................................................................3
4. Information security requirements ...........................................................................................3
5. Good practices ............................................................................................................................3
6. Acceptable use of ICT resources ...............................................................................................3
7. Unacceptable use of ICT resources ............................................................................................4
8. Personal Use ..................................................................................................................................5
9. Email Use ......................................................................................................................................5
10. Information Security ..................................................................................................................6
11. ICT equipment standard.............................................................................................................6
12. Copyright, licenses, software ........................................................................................................6
13. ICT Equipment Procurement.....................................................................................................6
14. Acceptable Internet Usage ..........................................................................................................6
14. Unacceptable Internet Usage ......................................................................................................7
15. Authority over equipment ............................................................................................................8
16. Grant and gift ...............................................................................................................................8
17. Handover ......................................................................................................................................8
18. Repair and maintenance .............................................................................................................8
19. Enforcement and processes .........................................................................................................8
1. Introduction

Information and Communication Technology (ICT) Section is a growing sector within the Bangladesh Red Crescent Society. The Society wants to deliver its services to the beneficiaries by means of state-of-the-art information technology tools and applications. Process automation and implementing mission-critical ICT solutions is a key focus of the Section in enabling BDRCS to become a fully automated and well-functioning National Society as far as using technologies is concerned to deliver with efficiency.

ICT section of BDRCS have plan to support the staff, volunteers, community as per alignment with govt. ICT sector to provide technical, technological and device support with digital facilities to HR and volunteers. To achieve the mission and goal BDRCS recognized and appreciate use of information and communication technology (ICT) in its day to day work. For ensuring the best use of ICT, minimize cost, maintenance time and stop pilferage this policy applies to all the officials and user of equipment, tools software or hardware, knowledge and other resource belongs to BDRCS.

2. Objective

This document outlines the policy on what users should and should not do to implement adequate information security controls and to ensure that the use of ICT resources is effective, efficient and consistent with the Fundamental Principles of the RCRC movement.

3. Applicability & Scope

This policy applies to all users including the contractual staff of Bangladesh Red Crescent Society.

It is applicable to information / data assets in whatever form, including, but not limited to, hard copies of documents, electronic data, images, the spoken word, computer equipment, network or data communication equipment, computer programs, procedures and support software, data storage devices and media.

4. Information security requirements

All users are responsible for enforcing appropriate controls to mitigate security risks regarding information or data that they access, handle or use, and report information security breaches.

As set out in the Information Classification Standard, appropriate controls are defined according to the category of the information / data being used, which is specified by the information asset owner on the information / data asset itself, whatever the form is (document, electronic).

5. Good practices

Users are advised to follow the general rules below, to minimize information security risks:

I. Users should not store information on their local drive (C:\) or the PC desktop. Saving to the desktop hinders flexible working and slows the log in process.

II. When taking on temporary or casual staff, managers should consider what system and data folders these users will need to access, to perform their duties, before asking the Service Desk to set them up on the network.

III. Users should lock their computer when leaving their desk unattended for short time, or log out when they are likely to be away for a longer period.

6. Acceptable use of ICT resources

Use of the BDRCS’s ICT resources is granted in accordance with the following principles:
I. ICT resources may only be used for legitimate purposes related to the activities of the BDRCS. When using ICT resources, users must uphold and promote the highest standards of ethical and professional conduct. Inappropriate use of ICT resources may result in disciplinary action up to and including dismissal.

II. ICT resources must be used consistently with the Fundamental Principles of the Movement, with this Policy, and with the Staff Code of Conduct.

III. Users are responsible for the safe keeping of any ICT equipment provided to them (like laptops or mobile phones). Any loss of such equipment must be reported to the ISD Service Desk as soon as possible with details of the data stored on the equipment.

IV. Use of ICT resources must comply with any applicable national or international laws governing computer fraud, pornography, misuse of equipment/resources, privacy of information, and related criminal offences, and any other legal requirements, such as copyright and licensing obligations.

V. Use of ICT resources may be monitored for security, network management or other reasons, and may be subject to use limitations.

7. Unacceptable use of ICT resources

Any use of ICT resources for purposes that are offensive, unlawful or otherwise contrary to the Code of Conduct, this Policy, Staff Regulations or HR policies is unacceptable. For example, the following activities are unacceptable and are prohibited:

I. Using BDRCS ICT resources inconsistently with the Code of Conduct or this Policy.

II. Intentionally visiting internet sites, downloading, emailing, or otherwise accessing material that is indecent, pornographic, hateful or otherwise objectionable (unless specifically required as part of their work). Accessing such material may constitute gross misconduct and may result in summary dismissal.

III. Attempting to defeat system security, attempting to access unauthorised data, or making unauthorised changes to data.

IV. Using ICT resources with a false or someone else’s identity (unless required for work purposes – e.g. to test information systems).

V. Using or installing non-standard devices or non-tolerated software. All use of information systems must be consistent with BDRCS’s contractual obligations, including limitations defined in software and other licensing agreements.

VI. Users must not set up any Outlook rules to forward e-mail to their home e-mail addresses or any other non-BDRCS address. This minimizes the risk of sensitive material being forwarded to insecure mail systems.
VII. Using ICT resources in violation of civil or criminal law. Users should be aware that this includes breaching copyright laws. Copyright laws govern the copying, display, and use of software and other works in digital form.

8. Personal Use

The BDRCS allows limited reasonable personal use of ICT resources by users. The BDRCS is solely responsible for determining what usage is "reasonable", taking into account the relevant circumstances. The BDRCS can impose limits on, or end, such personal use if it considers that to be appropriate. ICT resources are provided for work purposes.

Personal use must not interfere with the operation of the network, hinder or distract other users in their work. Personal use must also not result in any additional cost or liability for the BDRCS. Personal use must not materially detract from the ability of a user to undertake their assigned work. Examples of activities that are likely to impact on the BDRCS (whether in terms of cost, network capacity or otherwise) include: personal telephone calls, high data usage services (such as video or data streaming), video conferencing for personal purposes, playing interactive games, downloading large personal files, and interactive message services. Should a user member be unaware of the potential impact of his or her usage, and then he or she should seek advice from ICT section.

While the BDRCS allows users to occasionally use BDRCS computer systems (within reasonable limits) for the storage of personal files or the transmission of personal messages, this is a convenience allowed to users as a courtesy and at their own risk. The BDRCS cannot guarantee the privacy of such files or messages and may limit or stop such activities as it considers necessary.

9. Email Use

Users must be aware that whenever they send an email under the “___BDRCS.org” address they are representing the BDRCS. Emails can legally bind the BDRCS and can expose the BDRCS to legal liability and damage to reputation. Users must therefore ensure that the highest ethical standards are adhered to.

Examples of unacceptable email practices include: “flaming” (i.e. responding in an outright negative and inflammatory manner by email), circulating spam/junk mail or “chain” emails, impersonating another email user, and sending offensive or objectionable emails.

Users should implement appropriate information security controls and follow good email practice, such as archiving, minimizing attachment size, and minimizing use of “reply to all” when not necessary. Personal emails and files should be not be archived on the system longer than what is strictly necessary. Emails sent or received as official communications are BDRCS records and must be retained for as long as they are needed for BDRCS administrative and legal requirements.
10. Information Security
All electronic information (personal or official) sent or stored on BDRCS ICT resources are the property of the BDRCS. The BDRCS reserves the right to access, read, and act upon, all such information, including all emails and SMS messages sent or received through BDRCS ICT resources.

Users are responsible for maintaining the security of their own information system accounts and passwords.

- For passwords, users should avoid using words that can be associated with them (e.g. names or dates of birth).
- Password(s) should be memorized, and should not be written down or shared with others.

Users should be aware of the dangers posed to ICT systems from viruses and other malicious entities. Users should take reasonable precautions to protect ICT resources by:

- Ensuring that ICT resources under their control are regularly updated against malicious code, and
- Ensuring that removable media is scanned for viruses before use in BDRCS’s equipment.

11. ICT equipment standard
ICT section would create an ICT equipment and software standard for BDRCS which will be valid for two years. The standardization process may include review of similar document of other movement partners and other GO, INGO, market survey, statistic of different benchmarking organization, statistic found from international customer review sites. The document can be updated or changed in response of major product changes and current status of the local market.

12. Copyright, licenses, software
The BDRCS’s policy is to purchase sufficient licenses for users to undertake their work. ICT section will regulate the licenses in standard software provided with BDRCS equipment. Any nonstandard software loaded on BDRCS computers must be properly licensed and authorised. Users must ensure that license documentation is available.

Users wishing to load software on their computer must follow the relevant BDRCS policies and procedures, available from ICT section.

13. ICT Equipment Procurement
All the IT/ICT related equipment should be procured following the technical specification recommended by the ICT section. The section has the authority to change the specification that best serves BDRCS. In the process of CBA (Competitive Bid Analysis) the priority list will be on the following order manufacturer, soul distributor, renowned supplier and minimum price.

14. Acceptable Internet Usage
Employees are expected to use the Internet responsibly and productively. Internet access is limited to job-related activities only and personal use is not permitted.

Job-related activities include research and educational tasks that may be found via the Internet that would help in an employee’s role.

All Internet data that is composed, transmitted and/or received by BDRCS’s computer systems is considered to belong to BDRCS and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties.

The equipment, services and technology used to access the Internet are the property of BDRCS and the BDRCS reserves the right to monitor Internet traffic and monitor and access data that is composed, sent or received through its online connections.

Emails sent via the BDRCS email system should not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of vulgar or harassing language/images.

All sites and downloads may be monitored and/or blocked by BDRCS if they are deemed to be harmful and/or not productive to business.

The installation of software such as instant messaging technology is strictly prohibited.

### 14. Unacceptable Internet Usage

Accessing pornographic/vulgar/erotic contents in any format.

Viewing video contents without official purpose for a long time causing network overload.

Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via <BDRCS's> email service.

Using computers to perpetrate any form of fraud, and/or software, film or music piracy.

Stealing, using, or disclosing someone else's password without authorization.

Downloading, copying or pirating software and electronic files that are copyrighted or without authorization.

Sharing confidential material, trade secrets, or proprietary information outside of the organization.

Hacking into unauthorized websites.

Sending or posting information that is defamatory to the BDRCS, its products/services, colleagues and/or customers.

Introducing malicious software onto the BDRCS network and/or jeopardizing the security of the organization's electronic communications systems.
Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities

Passing off personal views as representing those of the organization.

If an employee is unsure about what constituted acceptable Internet usage, then he/she should ask his/her supervisor for further guidance and clarification.

All terms and conditions as stated in this document are applicable to all users of BDRCS's network and Internet connection. All terms and conditions as stated in this document reflect an agreement of all parties and should be governed and interpreted in accordance with the policies and procedures mentioned above. Any user violating these policies is subject to disciplinary actions deemed appropriate by BDRCS.

15. Authority over equipment

All the ICT equipment irrespective of procurement funding source or activity belongs to BDRCS. The ICT section process the right over all the ICT equipment of BDRCS to be:

I. Hand over and reclaim.
II. Swap between activity/department/user.
III. Require for repair and maintained.

16. Grant and gift

All the gift and grants of ICT equipment from any party to BDRCS should be handed over to the ICT section. The section has the right:

a) To receive or reject the equipment if they do not comply with the minimum standard for ICT equipment set by BDRCS, too old or broken.

b) To distribute received equipment as per need that benefits the organization best.

17. Handover

Any ICT equipment handover irrespective of temporary or permanent should be acknowledge and authorised by the ICT section. Proper documentation should be followed in any case of handover process which includes handover note and up gradation of the ICT inventory.

18. Repair and maintenance

The repairing and maintenance of any ICT equipment should be carried out as per the advice of ICT section, the cost of replacement of any parts shall be charged to the user department/section/activity.

19. Enforcement and processes
The BDRCS values privacy and confidentiality, and recognizes the interest of individuals in protecting information held in BDRCS’s ICT systems from unauthorized access. Even so, there are circumstances which may outweigh a user's privacy interests and warrant the BDRCS accessing relevant ICT resources without the knowledge and/or consent of the user.

Those circumstances include situations:

- when it is necessary to identify or diagnose systems or security vulnerabilities and problems, or otherwise preserve the integrity of the ICT resources,
- when there are grounds to believe that a breach of BDRCS’s regulations, rules, or policies may have taken place and access to such systems may reveal information relevant to an investigation of possible misconduct,
- when such access to information systems is required to carry out essential BDRCS business functions.

Access to such information without the knowledge and/or consent of users requires the approval of the Heads of the ISD and Human Resources Departments (or their delegates), except when access is required by managers, to preserve the integrity of facilities. In addition to accessing the information systems, the BDRCS may deactivate or limit a user's access privileges to ICT resources.

**Sanctions**

Users are accountable for any breaches of this Policy. Violations of this policy and related policies, standards, procedures and regulations may be subject to disciplinary measures, as appropriate. Contractors that violate BDRCS policies, standards, procedures and/or regulations may have their contract with BDRCS terminated. In addition, BDRCS reserves the right to recover from “users” all expenses incurred by BDRCS as a result of any violation of this Policy (including remedying harms, costs, etc.).

BDRCS July 2018

**STATEMENT OF RECEIPT**

I declare that I have received, read and understood the BDRCS’s ICT Policy. I understand that this Policy forms part of my conditions of service with the BDRCS and I agree to abide by its terms.

Signature  ________________________________
Name  ________________________________
Place  ________________________________