International Federation
of Red Cross and Red Crescent Societies

Information Security: Acceptable Use Policy

Document reference number:062

Document authorization				
Stakeholder	**Name**	**Position**	**Signature**	**Date approved**
Author	Ed Happ	Head, Information Systems Department		20.12.2013
Document owner	Michael Veltman	Head, Human Resources Department		19.02.2014
Document authorizer	Malika Ait-Mohamed Parent	USG, GMS		20.12.2013
Document authorizer	Matthias Schmale	USG, NSKD		20.12.2013
Document stakeholders	Sayed Hashem	Head, Risk Management and Audit Department		20.12.2013
Document stakeholders	Elise Baudot	Head, Legal Department		20.12.2013

Version number:2.5
Authorization date:19.02.2014
Document classification: internal

Document Control

This document is subject to change control and any amendments to main versions will be recorded below.

Change History

Version	Date	Notes
1.0	October 2007	First version of the policy
2.1	7 June 2013	Revised policy
2.2	17 June 2013	Revised draft incorporating comments received by 14.06.2013 from project stakeholders
2.3	2 July 2013	Revised draft incorporating comments received by 01.07.2013 from project stakeholders
2.4	15 July 2013	Revised draft incorporating comments received by 12.07.2013
2.5	29 July 2012	Revised draft incorporating comments received by 26.07.2013

Version Awareness

The audience of this document should be aware that a physical copy may not be the latest version available. The latest version which supersedes all previous versions is available on FedNet.

Glossary

Availability: Ability of a user to access information in a specified location and in the correct format when he needs it.

Clear desk policy: A policy that requires "staff" to clear desks of all papers at the end of the day, before leaving the office.

Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Employee: The term employee refers to a subset of IFRC staff. It includes Geneva-based staff and delegates (see IFRC's staff rules and regulations).

Information asset: Identifiable collection of information, stored in a manner (electronic, printed) and recognized as having value for the purpose of enabling the organisation to perform its business functions.

Information asset owner: Person or group of persons who have been identified as being responsible to ensure confidentiality of information asset. By default, unless specified otherwise, the information asset owner will be the manager responsible for that information.

Information classification categories: Information classification categories define, based on specific criteria, how information has to be classified.

Information classification controls: Information classification controls define how information assets, based on their classification, have to be handled.

Information integrity: The safeguarding of information accuracy and completeness over its entire life-cycle.

Information security: Information security is the process of protecting data whether in storage, transit or processing from unauthorized access, use, disclosure, destruction, modification, or disruption whether accidental or intentional. The information security processes ensure the confidentiality, integrity and availability of information.

Need-to-know principle: access should be restricted to the minimum number of persons who need it for the conduct of their official duties

Personally Identifiable Information (PII): PII refers to information, which by itself or combined with other information, can be used to identify, contact, or locate a person (e.g. name, email, birth date, passport number, social insurance number, criminal record, etc.).

Retention period: IFRC records are to be disposed of in accordance with the relevant Department's approved records retention and disposal schedule (see IFRC's filing categories and retention disposal instructions on FedNet for more details).

Staff: The term staff refers to IFRC employees (Geneva-based staff and delegates), local staff, consultants, volunteers, and interns, as well as staff-on loan and all individuals working under the IFRC name and legal status (see IFRC's Code of Conduct).

Users: In this document, the term users refers to all IFRC "staff", contractors and third party suppliers authorized to access, handle or use IFRC information or data.

Table of Contents

1. Introduction

The International Federation of Red Cross and Red Crescent Societies (IFRC) uses the information it receives and handles in a number of different ways. IFRC's reputation, and the effectiveness and efficiency of what it does, can be put at considerable risk if users – i.e. all IFRC "staff[1]", contractors and third party suppliers authorised to access, handle or use IFRC information – fail to maintain proper standards and controls in the way they manage information security.

The IFRC's Information Systems Department (ISD) is responsible for maintaining the security and integrity of the IFRC's information and communications systems. With the Human Resources Department, it ensures user awareness of IFRC's information security framework[2] and of users' expected standards of conduct regarding the use of Information and Communications Technologies (ICT) resources.[3] ISD is also responsible for ensuring that necessary action is taken if those standards are not met.

2. Objective

According to IFRC's information security framework, this Policy sets out what users should and should not do, to:

- implement adequate information security controls, and
- ensure that the use of ICT resources is effective, efficient, and consistent with the Fundamental Principles of the Red Cross / Red Crescent Movement

3. Applicability & Scope

The information security framework, including this Policy, applies to all users. This Policy also applies to Participating National Societies (PNS) and Host National Societies (HNS) that have signed an agreement with IFRC, and fall under the IFRC's security responsibility, including abiding by its Code of Conduct. National societies that are not integrated with IFRC delegations in the field are not covered by the Acceptable Use Policy, and should only be provided guest access to the network, unless they sign this Policy.

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 to relevant IFRC managers.[4]

[1] See the glossary for a definition of "staff".
[2] See the Information Security Charter for more details
[3] For the purposes of this Policy, ICT resources include hardware such as desktops, laptops, notebooks, mobile devices and satellite telephones, any related applications, data and software licensed to or owned by the IFRC.
[4] See the Information Security Charter for more information on roles and responsibilities,

As set out in the Information Classification Standard[5], appropriate controls are defined according to the category of the information / data being used, which is specified by the information asset owner[6] on the information / data asset itself, whatever the form is (document, electronic).[7]

5. Good practices

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

- 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. Moreover, it leads to a risk of data loss, as ISD does not make any back-up of the local drive or desktop.
- 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.
- 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 IFRC's ICT resources is granted in accordance with the following principles:

1. ICT resources may only be used for legitimate purposes related to the activities of the IFRC. 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.

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

3. 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.

4. 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.

5. 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:

1. Using IFRC ICT resources inconsistently with the Code of Conduct or this Policy.

[5] See the Information Classification Standard on FedNet. Information classification controls are also copied in the Annex of the document.
[6] See the glossary for a definition of "information asset owner".
[7] See the Information Classification Standard for more details.

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

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

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

5. Using or installing non-standard devices or non-tolerated software.[8] All use of information systems must be consistent with IFRC's contractual obligations, including limitations defined in software and other licensing agreements.

6. Users must not set up any Outlook rules to forward e-mail to their home e-mail addresses or any other non-IFRC address. This minimizes the risk of sensitive material being forwarded to insecure mail systems.

7. 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 IFRC allows limited reasonable personal use of ICT resources by users. The IFRC is solely responsible for determining what usage is "reasonable", taking into account the relevant circumstances. The IFRC 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 IFRC. 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 IFRC (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 ISD staff.

While the IFRC allows users to occasionally use IFRC 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 IFRC cannot guarantee the privacy of such files or messages and may limit or stop such activities as it considers necessary.

9. Use of Email

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

[8] See the IT system exception checklist at https://servicedesk.ifrc.org

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 IFRC records and must be retained for as long as they are needed for IFRC administrative and legal requirements.

10. Security

All electronic information (personal or official) sent or stored on IFRC ICT resources are the property of the IFRC. The IFRC reserves the right to access, read, and act upon, all such information, including all emails and SMS messages sent or received through IFRC 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 memorised, 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 IFRC’s equipment.

11. Copyright, Licenses and Software

The IFRC’s policy is to purchase sufficient licenses for users to undertake their work. ISD will regulate the licenses in standard software provided with IFRC equipment. Any nonstandard software loaded on IFRC 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 IFRC policies and procedures, available from ISD.

12. Enforcement and Processes

The IFRC values privacy and confidentiality, and recognizes the interest of individuals in protecting information held in IFRC’s ICT systems from unauthorized access. Even so, there are circumstances which may outweigh a user's privacy interests and warrant the IFRC 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 IFRC'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 IFRC 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 IFRC 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 in accordance with the Chapter IX of Staff Regulations for Employees or local staff regulations, as appropriate. Contractors that violate IFRC policies, standards, procedures and/or regulations may have their contract with IFRC terminated. In addition, IFRC reserves the right to recover from "users" all expenses incurred by IFRC as a result of any violation of this Policy (including remedying harms, repatriation costs, etc.).

IFRC AUP December 2013

STATEMENT OF RECEIPT

I declare that I have received, read and understood the IFRC's Information Security: Acceptable Use Policy. I understand that this Policy forms part of my conditions of service with the IFRC and I agree to abide by its terms.

Signature _____

Name _____

Place _____

Date _____

Annex: Information Classification Controls[9]

This section contains summary details of the controls relevant for the various security classification levels. All relevant IT procedures, standards and guidelines remain applicable at any time for all electronic data.[10]

Highly restricted

INFORMATION LIFECYCLE		"HIGHLY RESTRICTED" Controls
Use & modification	Format change	Information should not be duplicated to another format unless protected as required (i.e. integrity of the information format should be preserved, for example using non-changeable PDF files).
Distribution	Manual transmission of documents	✓ An opaque envelope has to be used. ✓ Delivery is only permitted by a messenger that has been approved by the owner of the document/data. ✓ Signed acknowledgment of receipt should be required.
	Electronic transmission of data	✓ All data transmission must be done through a highly secure authenticated messaging application. It cannot be done through regular email – whether corporate or personal. ✓ Data can only be transmitted to individual recipients (i.e. no distribution list) and cannot be forwarded to other recipients. ✓ Electronic acknowledgment of receipt should be required ✓ Highly restricted information should not be transmitted by fax. ✓ Printer(s) should not be left unattended while "highly restricted" documents are being printed out. ✓ Information assets are only printed by using a secure printing option.
	Spoken words	✓ Must occur behind closed doors in fully enclosed rooms. Unless not possible otherwise, it is highly recommended not to transmit that data by phone. ✓ Highly restricted information should not be transmitted by radio. ✓ Information must be removed from equipment and/or whiteboards prior to leaving the room.
	Copying	✓ Should be kept to a minimum in accordance with operational requirements.
Storage	Physical storage	✓ Documents should be stored in locked cabinets or drawers to prevent unauthorized access. ✓ When travelling, highly restricted data should be kept with the traveller at all times (i.e. it should not be in the checked in luggage).

[9] See the Information Classification Standard on FedNet for more details
[10] See IT procedures, standards and guidelines on FedNet for more details.

INFORMATION LIFECYCLE		"HIGHLY RESTRICTED" Controls
	Electronic storage	✓ Access should be restricted to the minimum number of persons who need it for the conduct of their official duties (i.e. on a need to-know-basis). ✓ Data is systematically secured (i.e. encrypted). ✓ Data can only be stored on a secure device / location (e.g. encrypted USB key) with appropriate access restrictions. This data needs to be backed-up in a secure location with equal or higher security level and access restrictions. ✓ Highly restricted data cannot be stored in locations where IFRC has no control over data and may be subject to government interference (e.g. Dropbox, Google drive).
Backup	Electronic	✓ Access to backups is restricted to minimum. ✓ Restore of backups is only permitted upon formal request and validation from the information owner ✓ Restore of backups is only made accessible to the information owner.
Disposal	Paper	✓ Documents and related working papers that are to be destroyed when their retention period[11] is completed must be shredded in a timely and secure manner. ✓ Documents and related working papers that are to be transferred to IFRC's Archives for permanent storage when their retention period is completed must be transferred to IFRC's Archives in a timely and secure manner.
	Electronic	✓ All media must be physically destroyed or sanitized when retention period is over. Electronic documents that are to be transferred to IFRC's Archives for permanent storage when their retention period is completed must first be printed and the printed version transferred to IFRC's Archives in a timely and secure manner, then the electronic media must be physically destroyed or sanitized.

Restricted

INFORMATION LIFECYCLE		"RESTRICTED" Controls
Use & modification	Format change	✓ Information should not be duplicated to another format, unless protected as required (i.e. integrity of the information format should be preserved, for example using non-changeable PDF files).
Distribution	Manual transmission of documents	✓ An opaque envelope has to be used when sending documents (such as personnel records) by post or courier service between IFRC offices (e.g. field office and Geneva).
	Electronic transmission of data	✓ Electronic data transmission can be done by corporate email, but should be protected from access by unauthorized users. ✓ Data can be transmitted to distribution lists. ✓ Electronic message can be forwarded to other recipients if they need to know the information concerned. Printer(s) should not be left

[11] See the glossary for a definition of "retention period".

INFORMATION LIFECYCLE		"RESTRICTED" Controls
		unattended while "Restricted" documents are being printed out or faxed. ✓ Electronic acknowledgment of receipt should be required.
	Spoken words	✓ Must occur behind closed doors in fully enclosed rooms. Unless not possible otherwise, it is highly recommended not to transmit that data by phone. ✓ Restricted information should not be transmitted by radio. ✓ Information must be removed from equipment and/or whiteboards prior to leaving the room.
	Copying	✓ Should be kept to a minimum in accordance with operational requirements.
Storage	Physical storage	✓ Documents should be stored in locked cabinets or drawers to prevent unauthorized access. ✓ When travelling, restricted data should be kept with the traveller at all times (i.e. it should not be in the checked in luggage).
	Electronic storage	✓ Access should be restricted to the minimum number of persons who need it for the conduct of their official duties (i.e. on a need-to-know basis). ✓ Data can only be stored on a secure device / location (e.g. encrypted USB key) with appropriate access restrictions. This data needs to be backed-up in a secure location with equal or higher security level and access restrictions. ✓ Restricted information can be stored outside of IFRC premises with appropriate security controls
Backup	Electronic	✓ Access to backups is restricted to minimum. ✓ Restore of backups is only permitted upon formal request and validation from managers.
Disposal	Paper	✓ Documents and related working papers that are to be destroyed when their retention period is completed must be shredded in a timely and secure manner. ✓ Documents and related working papers that are to be transferred to IFRC's Archives for permanent storage when their retention period is completed must be transferred to IFRC's Archives in a timely and secure manner.
	Electronic	✓ All media must be physically destroyed or sanitized when retention period is over. Electronic documents that are to be transferred to IFRC's Archives for permanent storage when their retention period is completed must first be printed and the printed version transferred to IFRC's Archives in a timely and secure manner, then the electronic media must be physically destroyed or sanitized.

Internal

INFORMATION LIFECYCLE		"INTERNAL" Controls
Use & modification	Format change	✓ No restriction
Distribution	Manual transmission of documents	✓ No restriction
	Electronic transmission of data	✓ Corporate email addresses should be used for the first distribution of internal information (i.e. use @ifrc.org emails).[12] ✓ No restriction for the printing or faxing or internal information
	Spoken words	✓ No restriction
	Copying	✓ No restriction
Storage	Physical storage	✓ "Clear desk" policy is systematically applied – i.e. internal documents should not be left on desks without monitoring, when staff leaves the office.
	Electronic storage	✓ Access is restricted to internal users
Backup	Electronic	✓ Access to backups is restricted to minimum.
Disposal	Paper	✓ Documents and related working papers that are to be destroyed when their retention period is completed must be shredded in a timely and secure manner. ✓ Documents and related working papers that are to be transferred to IFRC's Archives for permanent storage when their retention period is completed must be transferred to IFRC's Archives in a timely and secure manner.
	Electronic	✓ All media must be physically destroyed or sanitized when retention period is over. Electronic documents that are to be transferred to IFRC's Archives for permanent storage when their retention period is completed must first be printed and the printed version transferred to IFRC's Archives in a timely and secure manner, then the electronic media must be physically destroyed or sanitized.

[12] Participating National Societies (PNS) or Host National Societies (HNS) integrated with an IFRC delegation would then be responsible for the subsequent distribution of relevant internal information.

Public

INFORMATION LIFECYCLE		"PUBLIC" Controls
Use & modification	Format change	✓ No restriction
Distribution	Manual transmission of documents	✓ No restriction
	Electronic transmission of data	✓ No restriction for the electronic transmission - including printing and faxing - of public information
	Spoken words	✓ No restriction
	Copying	✓ No restriction
Storage	Physical storage	✓ No restriction
	Electronic storage	✓ No restriction
Backup	Electronic	✓ No restriction
Disposal	Paper	✓ Documents and related working papers that are to be destroyed when their retention period is completed must be shredded in a timely and secure manner. ✓ Documents and related working papers that are to be transferred to IFRC's Archives for permanent storage when their retention period is completed must be transferred to IFRC's Archives in a timely and secure manner.
	Electronic	✓ All media must be physically destroyed or sanitized when retention period is over. Electronic documents that are to be transferred to IFRC's Archives for permanent storage when their retention period is completed must first be printed and the printed version transferred to IFRC's Archives in a timely and secure manner, then the electronic media must be physically destroyed or sanitized.