Information Classification Policy

Document reference number: 200

Document authorization				
Stakeholder	**Name**	**Position**	**Signature**	**Date approved**
Author	Tamas Foldesi	Senior Officer, IT Security, Policies, Quality		
Document stakeholder	Sylvia Gil	Director, DITD		
Document stakeholders	Sayed Hashem	Director, Internal Audit, and Investigations Department		
Document stakeholders	Lucie Laplante	General Counsel		
Document authorizer	Nena Stoiljkovic	USG – Global Relations, Humanitarian Diplomacy, Digitalisation		
Document owner	Jagan Chapagain	Secretary General		

Version number: 2.02
Authorization date: 20th November 2020

IFRC Internal

Table of contents

1. Purpose, scope and audience

This policy defines the information security classification of information assets, based on their sensitivity level, and on the impact that the unauthorized access, disclosure, alteration, destruction or other misuse of those information assets would have on the organization. The aim is to help users determine the criticality of the information asset, which will then drive the security controls implemented around them.

The information security framework – including this information security classification policy – applies to all information owners. However, since information owners may delegate their responsibilities organization-wide to other users, including IFRC staff, contractors and third-party suppliers authorized to handle IFRC information, any time during and after their service with IFRC, all above listed individuals are required to abide to this IFRC information security classification policy. From an information classification perspective, ICRC and national societies are third parties and information sharing with them may be subject to contractual terms between the parties.

The information classification policy is applicable to:

- Any IFRC information assets in whatever form, including, but not limited to hard copies, electronic data, including images, audio files, electronic documents, electronic records, database records, the spoken word, etc.
- their storage and transmission equipment in whatever form, including, but not limited to computer equipment, network or data communication equipment, paper file cabinets, computer programs, procedures and support software, data storage devices and media.

2. Information Classification Framework

2.1 Classification Categories

All information assets are classified in one of the following five information categories, according to their sensitivity level: highly confidential, confidential, internal, restricted, or public. Any unclassified information asset is per default considered as being “highly confidential”, until it has been classified.

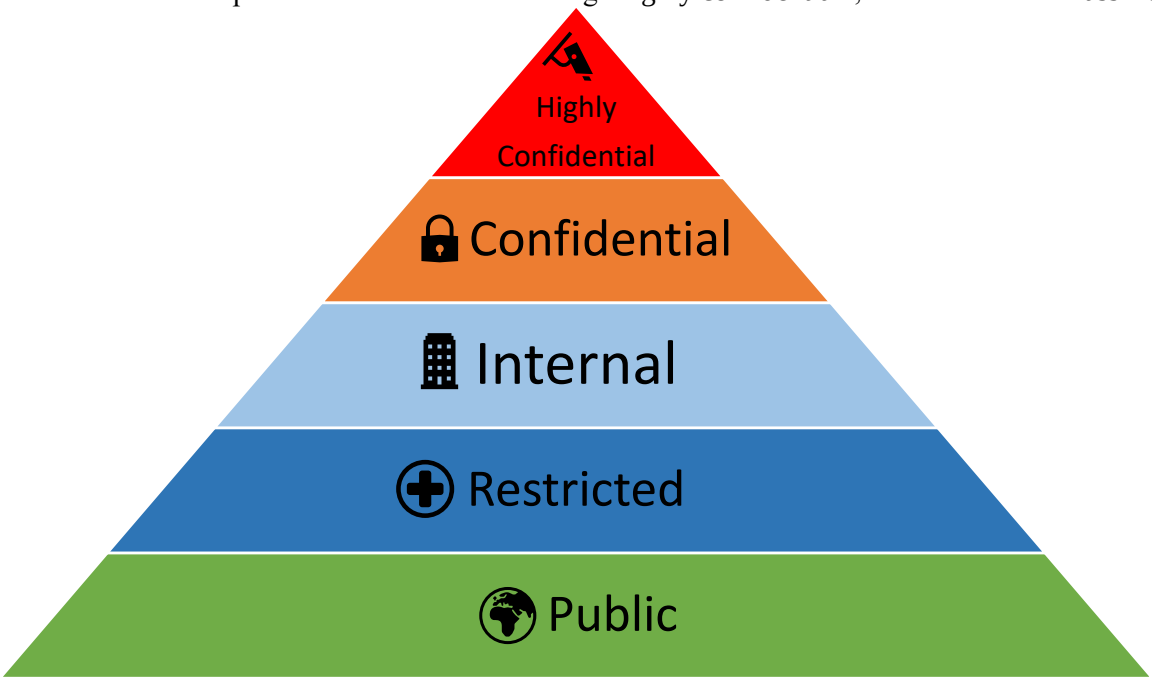

Figure 1. IFRC Information classification categories

2.2 Definition of categories

2.2.1 Highly Confidential

This category was previously classified as 'highly restricted'. Unauthorized disclosure, alteration or destruction of Highly Confidential information (example: mass disclosure of health and location records of beneficiaries during an Ebola outbreak) could have severe or catastrophic impact on IFRC's operations, its capacity to work in accordance with Fundamental Principles of the Red Cross / Red Crescent, on beneficiaries or on partners, due to one or more of the following potential impacts:

2.2.1.1 Health and safety impact

- Beneficiaries or staff in danger of serious injury or death.
- Catastrophic environment incident (ISO14000)

2.2.1.2 Financial impact

- High penalty costs (above 5% of the specific budget)
- High recovery costs (above 5% of the specific budget)
- Severe fraud, theft consequences (above 5% of the specific budget)

2.2.1.3 Operational impact

- Complete inability or severe impact on IFRC's capacity to assist people in need, and achieve its mission (target missed above 30%)
- Complete inability or severe impact on IFRC's work with National Societies, donors and other partners (target missed above 30%)

2.2.1.4 Reputational impact

- Worldwide negative publicity
- Complete loss of confidence
- Tangible drop in donations
- Legal actions against IFRC

2.2.2 Confidential

This category was previously referred to as 'restricted'. Unauthorized disclosure, alteration or destruction of Confidential information (example: disclosure of all IFRC staff financial/personal records active in a critical location, user IDs and passwords) could be expected to have a serious adverse impact on IFRC's operations, beneficiaries or its partners, due to one or more of the potential impacts below.

2.2.2.1 Health and safety impact

- Beneficiaries or staff at risk of being harmed.
- Moderate environment incident (ISO14000)

2.2.2.2 Financial impact

- Significant penalty costs (between 1% and 5% of the specific budget)
- Significant recovery costs (between 1% and 5% of the specific budget)
- Significant fraud, theft consequences (between 1% and 5% of the specific budget)

2.2.2.3 Operational impact

- Serious impact on IFRC's capacity to assist people in need, and achieve its mission (delivery 10%-20% below target)
- Serious impact on IFRC's work with National Societies, donors and other partners (delivery 10%-20% below target)

2.2.2.4 Reputational impact

- Regional negative publicity
- Significant loss of confidence

- Serious Drop in donations

2.2.3 Internal

Internal information is intended for the use of IFRC Secretariat staff, like internal procedures or training materials for example. The unauthorized disclosure, alteration or destruction of internal information could cause inconvenience to the organization or management, but is unlikely to result in serious financial loss or serious damage to IFRC operations:

2.2.3.1 Health and safety impact

- No Beneficiaries or staff at risk of being harmed.
- Insignificant environment incident (ISO14000)

2.2.3.2 Financial impact

- Limited or no penalty costs (up to 1% of the specific budget)
- Limited or no recovery costs (up to 1% of the specific budget)
- No fraud, theft consequences (up to 1% of the specific budget)

2.2.3.3 Operational impact

- Limited or no impact on IFRC's capacity to assist people in need, and achieve its mission (delivery 0-10% below target)
- Limited or no impact on IFRC's work with National Societies, donors and other partners (delivery 0-10% below target)

2.2.3.4 Reputational impact

- Local or no negative publicity
- No loss of confidence
- No drop-in donations

2.2.4 Restricted

Internal information is intended for the use of IFRC Secretariat staff, National Societies, contracted third parties, partner international organisations. Examples: security reports, travel advices or training materials for wider audience. The unauthorized disclosure, alteration or destruction of restricted information could be expected to be of minor inconvenience the organization or management, but is unlikely to result in any financial loss or serious damage to IFRC operations:

2.2.4.1 Health and safety impact

- No Beneficiaries or staff at risk of being harmed.
- No environmental impact at all.

2.2.4.2 Financial impact

- Limited or no penalty costs (up to 1% of the specific budget)
- Limited or no recovery costs (up to 1% of the specific budget)
- No fraud, theft consequences (up to 1% of the specific budget)

2.2.4.3 Operational impact

- Limited or no impact on IFRC's capacity to assist people in need, and achieve its mission (delivery 0-10% below target)
- Limited or no impact on IFRC's work with National Societies, donors and other partners (delivery 0-10% below target)

2.2.4.4 Reputational impact

- Local or no negative publicity

- No loss of confidence
- No drop in donations

2.2.5 Public

This category groups all information that IFRC has consciously and deliberately made available to the public. Disclosure of public information is not expected to have any negative effect on operations, assets, or individuals.

3. Responsibilities

The Secretary-General is the owner of this policy and is accountable for the implementation and control of information security throughout the IFRC Secretariat.

The information owner is accountable for the proper classification of the information. The information owner is also responsible to ensure the policy is known and understood by staff acting on their behalf.

On behalf of the information owner, the information author (or the recipient if the information originates from outside the IFRC) is responsible for classifying the information before it is released for further processing. S/he is also responsible for assigning an owner and keeping the owner aware of any further processing.

For additional information on the implementation of this Policy, please refer to the Information Handling Guidelines

4. Related documents

File number	Name	Version
245	Information Handling Guidelines	1.0

5. Document revision history

Version	Date	Details
0.1	29.05.2012	First draft
0.2	07.06.2013	Second draft incorporating comments received by 06.06.2013 from project stakeholders
0.3	17.06.2013	Third draft incorporating comments received by 14.06.2013 from project stakeholders
0.4	02.07.2013	Fourth draft incorporating comments received by 01.07.2013 from project stakeholders
0.5	15.07.2013	Fifth draft incorporating comments received by 12.07.2013
0.6	29.07.2013	Sixth draft incorporating comments received by 26.07/2013 from project stakeholders
1.0	20.12.2013	Final version after approval by heads of departments (ISD, Finance, HR, Legal, Audit) and USGs (Malika, Matthias)
2.0	27th of September 2018	Tamas Foldesi, document updated.
2.01	21st of January 2019	Tamas Foldesi, corrected 'Red Cross / Red Crescent Internal' label
2.02	20th of November 2020	Renamed label 'Red Cross / Red Crescent internal' to 'restricted'. As a result, 'IFRC internal' became simply 'internal'

Appendix 1: Non-exhaustive list of illustrative examples

Categories	Examples (Information owners are ultimately accountable for the right classification of their assets, any of the below typical examples may have various other classifications)
Highly confidential	• Vulnerable populations highly sensitive data with individual names (e.g. list of sexual workers with AIDS in highly sensitive countries) • Sensitive disciplinary process information as determined by the Human Resources and Legal departments • Fraud/corruption investigations • Information regarding kidnappings • Highly confidential audit reports • Certain legal matters as determined by the Legal department
Confidential	• Personally Identifiable Information (PII) regarding staff or beneficiaries: 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.) • Beneficiary data with individual names • Discussion on elections and appointments in Governance • Minutes of governance body meetings held in camera • Conversation with auditors • Procurement tender information (bids received from suppliers) • Supplier contractual information • Personnel files and work history data • Consultant contracts • Recruitment records of staff • Financial information (payroll, payments) • Financial statements until official release • Unverified or politically sensitive humanitarian or security incident information • Network architecture • Internal audit reports • Security incident reports
Internal	• Locations of warehouses, stocks and distribution sites, plans (exact address or GPS codes for stock locations or sites, dates when goods will be distributed) • Beneficiary data without individual names (e.g. general data about groups of population affected by aid) • Ordinary meeting agendas and minutes • Internal communications • Security assessment reports • Internal policies • Internal procedures • Internal standards • Financial documents read by active directory user • Supplier information (database of suppliers)
Restricted	• Reports, travel or security advices • Ordinary meeting agendas and minutes • Internal communications aiming at NS • Security assessment reports
Public	• External press releases and publications • Financial statements after release • Plan of action and Emergency Appeal, Development Plan documents (and all related updates and reports)