ICRC

INFORMATION HANDLING TYPOLOGY RULES

SECURITY MANAGEMENT

Information Handling Typology Rules (IHT Rules)

Published by:
Gil Talon & Brigitte Troyon (CIM-AIM)

Approved by:
The Information Security Board on 21 February 2017
The ICRC Directorate on 19 September 2017

IHT_RULES.DOCX

October 2017

DOCUMENT TYPOLOGY AND LIMITATION

The content of this document is the property of the ICRC. The content of this document is **public**.

All trademarks mentioned in this document are the property of the ICRC.

HISTORY

Updates			
Version	**Date**	**Author**	**Description**
1.0	January 2013	CIM_AIM_IM	First version
2.0-4.0	September 2016	CIM_AIM_IM	Revision 1 – Submitted to the Information Security Board
5.0	February 2017	CIM_AIM_IM	Submitted and approved by the Information Security Board
6.0	September 2017	CIM_AIM_IM	Submitted and adopted by the Directorate
7.0	October 2017	CIM AIM IM	Revised following the Directorate recommendations

The following Information Handling Typology Rules replaces Information Handling Typology (Annex 2) set out in the ICRC Information Environment: A Strategy for Information Management, Systems and Technology, adopted by the Assembly on 13 September 2012.

GLOSSARY

Assets	An asset is something that has value to an organization. There are tangible assets, such as offices, vehicles, machines or facilities, and non-tangible assets such as patents, software, services and information. Assets can also mean less obvious things such as people, reputation, image, skills or knowledge.
Authorized recipient	A natural person who is entitled to access specific information.
Beneficiary	Person to whom the ICRC is providing protection or assistance (a detainee, missing person, separated child, etc.)
Category of classification	"Public", "Internal", "Confidential" and "Strictly confidential" are the four categories.
Data	Data can be defined as something that is, or represents, a fact (Name, Birth Date, Indicators…)
Data controller	Means the natural or legal person, who, alone or jointly with others, determines the purposes and means of personal data processing.
Data processor	Means a person, public authority, agency or other body that processes personal data on behalf of the ICRC Controller. In certain cases, the ICRC is the processor when it processes personal data.
Data protection	Data protection is the framework designed to protect individuals' personal data, which is collected, processed and stored by a data controller. Data protection aims to safeguard individuals' fundamental right to privacy, which is enshrined in international, domestic and regional laws and conventions, as well as in the ICRC Rules on Personal Data Protection.
Data subject	Means an individual who can be identified, directly or indirectly, in particular by reference to personal data.
Handling rules	Govern the ways in which information must be treated.
Approved systems	IT Systems, software and hardware that have been approved for use by the ICRC (e.g. specific cloud service providers for data storage, smartphones, tablets and PCs). *See also* Non-approved systems.
Information	Information is data in context. Context means providing a meaning to the data, defending the format in which the data are presented and the relevance of the data within a certain usage context.
Information assets	The ICRC collects, processes, stores and transmits information via different forms of media, including electronic, physical and verbal. The term information assets covers all information and related processes, systems, networks and personnel involved in information processing and handling. Like other assets, they are valuable to an organization's work and consequently deserve or require protection.
Information lifecycle	Describes the different phases of a piece of information from creation, to dissemination or distribution to archiving.
Information Handling Typology (IHT)	The classification and handling rules for all information types (including documents, the spoken word, messages, chats, photos, videos, recordings, etc. and personal data).
Interlocutor	External entities or individuals with whom the ICRC engages in bilateral dialogue, such as authorities, donors, non-State armed groups.
Internal staff	Individuals working for the ICRC under an employment contract.
Need-to-know basis	The term "need-to-know basis" describes the restriction of information to those ICRC staff or other staff who have a specific *need to know*, i.e.

	access to the information is necessary for the conduct of their official duties.
Non-approved systems	IT systems, software and hardware that have not been approved for use by the ICRC. *See also* Approved systems.
External staff	Individuals working for or with the ICRC, or on its behalf, under any type of contract other than an employment contract or partnership agreement. This includes consultants, service providers, suppliers and partners (including National Society staff on secondment and staff from the Movement)
Owner of the information	The entity or natural person who has created **or** requested the creation of the information and is therefore accountable for its classification and the relevant handling rules.
Personal data	Personal data means any information relating to an identified or identifiable person. This may include an identifier such as a name or audio-visual materials, an identification number, location data or an online identifier; it may also mean information that is linked specifically to the physical, physiological, genetic, mental, economic, cultural or social identity of a data subject. The term also includes data identifying or capable of identifying human remains. Personal data processing is governed by the ICRC Rules on Personal Data Protection.
Processing	Means any operation or set of operations – by automated and other means – that is performed upon personal data or sets of personal data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, or erasure.
Recipient of the information	People who receive information. The recipient of the information must follow the requisite handling rules, depending on the category of classification as defined by the owner of the information.
Sensitive information	Information that unauthorized access or disclosure of, is likely to cause harm, such as discrimination or repression, to any natural person including the source of the information or other identifiable persons, beneficiaries, interlocutors, internal or external staff, or which may have a negative impact on the ICRC's capacity to carry out its internationally recognized mandate (access, dialogue, security) or its perception as a neutral, impartial and independent humanitarian actor. Sensitive information includes privileged information, sensitive personal data, information that must be protected by law, and information on the ICRC's internal or operational functioning that may not be shared publicly. Note that given the situations in which the ICRC works, what is considered sensitive information in one operational situation may not be sensitive in another. Consequently, a definitive list of what types of data constitute sensitive information is unlikely to be meaningful. However, taking into account the nature of data relating to the identity of the perpetrators and witnesses of violations, operational details related to military operations or security, health, race or ethnicity, religious/political/armed group affiliation, genetic and biometric data, there is a presumption that such categories of data fall under the definition of sensitive information at all times and, therefore, require additional protection.
Unauthorized recipient	An individual or entity that is not entitled to access certain information.

TABLE OF CONTENTS

1 BACKGROUND AND PURPOSE

A confidential approach is part of the ICRC's identity and implies protecting information as much as possible[1]. The ICRC **Rules on Personal Data Protection**[2] acknowledge that protecting personal data is an essential aspect of protecting people's lives, their physical and mental integrity, and their dignity. Being able to rely on available and relevant information is also one of the seven security pillars[3] that allows the ICRC to mitigate the inherent security risks it faces in its daily work.

The importance of protecting and maintaining the integrity of information and information systems is therefore vital to avoid loss of information assets, as well as to prevent unauthorized access to, and misuse or disclosure of, personal data and confidential information that could endanger ICRC staff, beneficiaries or other persons to whom the information relates. Information security incidents can have other far-reaching consequences for the organization, such as the disruption of operations and support functions affecting business continuity, financial losses in case of fraud, lawsuits brought against the ICRC by individuals or entities, failure to comply with the ICRC's legal obligations and reputational damage and loss of trust by staff, beneficiaries, interlocutors and donors.

To mitigate the security risks that have been mapped with respect to information,[4] the present Information Handling Typology Rules (IHT Rules) outline the criteria for classifying information and defining classification categories, and the handling rules to apply for all types of information. First and foremost, the owner of the information[5] must be clearly identified and must classify it, to enable recipients of the information to apply the appropriate handling rules.

This document complies with institutional policies, in particular with the Rules of the Code of Conduct related to the use of information technology, which constitute an integral part of an ICRC employment contract. The Information Handling Typology as well as the **Information Security Framework**, the ICRC Rules on Personal Data Protection,[6] the ICRC reference framework for managing documents and information (*Cadre de référence de la gestion des documents et de l'information au CICR*) and other specific guidelines on the security of ICRC information and information systems are binding on all staff.

2 SCOPE

Compliance with the following Information Handling Typology Rules is mandatory for all internal and external staff[7].

The IHT Rules apply:

- to all information in whatever form, including, but not limited to, hard copies of documents, electronic data, images, spoken words, computer equipment, network or data communication equipment, software, data storage, devices and media approved for use by the ICRC; and
- throughout the information lifecycle , i.e. from creation, transmission, dissemination to storage or destruction.

The Archive and Information Management Division is accountable for the implementation of the IHT Rules.

[1] Doctrine on the ICRC's confidential approach (policy document 58).

[2] ICRC Rules on Personal Data Protection.

[3] ICRC doctrine on the field security concept (policy document 16). The concept is based on the ICRC's seven pillars of security: acceptance of the ICRC, identification of the ICRC, information, security regulations, personality, telecommunications and protective measures.

[4] Risk Mapping/Assessment – Security Board – CIM_DIR

[5] *See* the definition of "Owner of the information" in the glossary.

[6] https://shop.icrc.org/publications/...law/icrc-rules-on-personal-data-protection.html.

[7] Staff that are no longer working for ICRC are bound by the duty of discretion and therefore must respect the IHT rules in tier public communication.

3 RESPONSIBILITY FOR CLASSIFICATION AND HANDLING OF THE INFORMATION

The owner of the information[8] is responsible for classifying information. To correctly classify information, all internal and external staff must take the following into account:

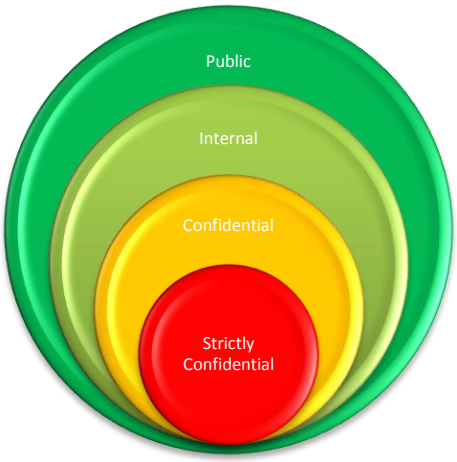
- The evaluation criteria as described in the table of classifications (Section 4.1 below).
- Any specific instructions by the 'métier' (functional managers) about information that requires specific attention (strictly confidential, confidential). Please refer to the Annex for specific examples.
- Any recommendations from line managers.
- Any recommendations from the Data Protection Office.

The classification category of a specific piece of information may change during its lifecycle. One of the most obvious cases is when archives become public after 50 or 70 years.[9] However, if information is to remain in a record closed to the public, its reclassification must be determined, or agreed by the owner.[10] The dissemination of the information, whatever its classification, remains the responsibility of the owner and the recipients of the information.

4 IHT FRAMEWORK

The IHT Rules apply throughout the lifecycle of information produced by – or in the possession of – the ICRC. There are four classification categories according to the sensitivity of the information:

- Strictly confidential[11]
- Confidential[12]
- Internal
- Public



All information must be classified. Information that is not classified will be considered "internal" by default and must be handled as such, unless the information falls under one of the categories defined in the Annex, or if caution guides the recipient to classify the information as "confidential" or "strictly confidential".

Internal, confidential and strictly confidential information may only be shared with external staff under certain circumstances and conditions (*see* Section 4.2 Handling Rules).

Please note that a Data Subject's right to access will be determined not by the category of classification, but pursuant to Article 8 of the ICRC Rules on Personal Data Protection.

[8] *See* the definition of the "Owner of the information" in the glossary.

[9] *See* the Rules governing access to the archives of the ICRC

[10] Reclassification of strictly confidential information stored in ICRC archives follows rules for declassification that were defined by the Archive and Information Management Division. For any information that has not been archived, rules on declassification will be the subject to a specific AIM division process. Until this process has been implemented, any reclassification should have the approval of the owner, or in his/her absence, his/her line manager.

[11] This term replaces the previous term "exceptional handling – strictly confidential".

[12] This term replaces the previous term "exceptional handling – confidential".

4.1 TABLE OF CLASSIFICATION

Type / Categories	Strictly confidential	Confidential	Internal	Public
Description	The unauthorized disclosure, alteration or destruction of this information could have a **severely adverse** impact on ICRC operations, assets, internal staff, external staff, beneficiaries or interlocutors.	The unauthorized disclosure, alteration or destruction of this information could have a **seriously adverse** impact on ICRC operations, assets or staff, external staff, beneficiaries or interlocutors.	Information which can be shared with internal and external staff and which must not be published in the public domain. Information that has not been classified is to be handled by default as if it were "Internal", unless it is clear that the information should have been classified as "Strictly confidential" or "Confidential".	This category of information concerns the ICRC's official public communications and information that is made available in the public domain by authorized persons (official channels for public information).
Consequences in case of disclosure, alteration or destruction	• Severe and long-lasting harm to the ICRC's capacity to protect, assist and act. • Severe risks to the ICRC's reputation, whether immediate or foreseen in the longer-term, either in a specific country or globally. • Severe risks for the safety of internal staff, external staff, beneficiaries, or interlocutors. • Severe invasion of employee privacy and serious impact on the social climate of part or all of the ICRC. • Physical or mental harm to internal staff, e external staff, beneficiaries, or interlocutors.	• Serious and lasting harm to the ICRC's capacity to protect, assist and act. • Serious risk to the ICRC's reputation, whether immediate or foreseen in the longer-term, either in a specific country or several countries. • Serious risks for the safety of internal staff, external staff, beneficiaries or interlocutors. • Possible impact on the social climate of part or all of the ICRC.	Risk of inconvenience for the ICRC, but unlikely to result in any **severely** or **seriously adverse** impact on its capacity to protect, assist and act.	No expected negative effect on the ICRC's capacity to protect, assist or act.

Type / Categories	Strictly confidential	Confidential	Internal	Public
Evaluation Criteria / Examples	• Information that contains sensitive personal data of internal staff, external staff, beneficiaries, interlocutors or other actors or any other identifiable individuals (Note that Personal Data must be treated pursuant to the ICRC Rules on Personal Data Protection). • Information which severely impacts the privacy of internal staff, external staff, beneficiaries, interlocutors or other actors (e.g. health, legal proceedings). • Medical files. • Information about a serious security and safety incident (abductions, sexual violence, killings, etc.) of internal staff or external staff. • Information on political or military situations which strongly affects the ICRC's capacity to act.	• Personal data of beneficiaries, internal staff, external staff, interlocutors or other actors whose disclosure may cause harm to ICRC, another entity or an individual. • Confidential dialogue with governments or non-State armed groups, including exchanges about violations of IHL. • Agreements with governments or non-State armed groups • Agreements with suppliers (contracts, tenders/offers). • Information which could impact the employment status of internal staff or external staff. • Information about security incidents, breaches, system weaknesses, etc. • Sensitive information which may impact on the ICRC's capacity to carry out its mandate.	• Personal data of beneficiaries, internal staff, external staff, interlocutors or other actors whose disclosure is unlikely to cause harm to the ICRC, another entity or to an individual. Only limited personal data of internal staff, external staff, beneficiaries, interlocutors or other actors (first name, last name, role, delegation name) on a need-to-know basis and in connection to an ICRC operation (e.g. no confidential HR data). • General or specific information (delegation/department/division/unit) for internal staff and/or external staff. • General information on activities, management, follow up, etc.	• Must not contain any personal data of the beneficiaries, internal staff, external staff, interlocutors or other actors or identifiable persons unless the Data Subject's consent has been obtained and/or a Data Protection Impact Assessment has been undertaken. • Information should be publicly available

4.2 HANDLING RULES

The following measures must be applied to protect information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction, and to ensure its confidentiality, integrity and availability.

	Strictly confidential	Confidential	Internal	Public
Access Level	Information is limited to specific members (authorized recipients) of internal staff on a need-to-know basis. External staff, beneficiaries, interlocutors and other actors should not have access to strictly confidential information except in exceptional cases duly documented (by contract or by obligation, for a limited period of time and on a need-to-know basis). Due to its **extremely sensitive content,** distribution of **strictly confidential** information is restricted, on a need-to-know basis, to a limited number of persons, who will be determined by the owner of the information.	Information is limited to a group of authorized recipients (internal staff, external staff, beneficiaries or interlocutors) on a need-to-know basis. Due to its **sensitive content**, distribution of **confidential information** is restricted on a need-to-know basis to a limited number of persons, which will be determined by the owner of the information.	Information is restricted to internal staff and external staff.	Information that is open to everyone, including outside the ICRC.
Access to information assets and systems	• Access to information assets requires a security check (identification badge for physical access to buildings and equipment, an ICRC account for login and secure encryption keys for electronic information, etc.). • Access is managed by the owner of the information. • Access is not allowed from non-approved systems.[13]	• Access to information assets requires a security check (identification badge for physical access to buildings and equipment, a secure login or secure encryption keys for electronic information). • Access is managed by the owner of the information. • Access is not allowed from non-approved systems.	• Access to information assets requires a security check (identification badge for physical access to buildings and equipment, a login or encryption keys for electronic information). • Access is managed by the owner of the information.	• The information must be sufficiently protected against unauthorized modification. • Access is allowed from non-approved systems.

[13] The list of **approved** systems is not a fixed one and will inevitably vary over time. A non-approved system could become an approved one and vice versa, hence the need to verify regularly if the system is approved or not.

	Strictly confidential	Confidential	Internal	Public
	• Recipients of strictly confidential information are not entitled to widen the distribution list without the authorization of the owner of the information.		• Access is not allowed from non-approved systems.	
Technical Protection / Storage	• Strictly confidential information is stored separately from other information, whether physically or in an electronic database. • Storage is secure (archives and paper files: storage in a locked safe; electronically stored information must only be accessible to authorized users with specific access). • Must not be stored in non-approved systems. *Sending strictly confidential information by email, SMS or instant messaging to a non-ICRC account is not secure. If regular electronic exchange of strictly confidential information is required, please contact the Service Desk for advice and support*.	• Storage is secure (archive and paper files: storage in a locked safe); electronically stored information must only be accessible to authorized users with specific access). Must not be stored in non-approved systems. *Sending confidential information by email, SMS or instant messaging to non-ICRC account is not secure. If regular electronic exchange of strictly confidential information is required, please contact the Service Desk for advice and support.*	• Archives: standard storage. • Must not be stored in non-approved systems	• Archives: standard storage. • Can be stored in non-approved systems.
Dissemination / Communication	• The information must not be communicated to unauthorized recipients in any form (i.e. in paper or digital form, or the spoken word, etc.). • All documents must bear a watermark with the category of classification "Strictly confidential" on every page. A property (metadata field) is used to classify the document as "Strictly confidential". • Photo, video, recording: a property (metadata field) is used to classify the asset as "Strictly confidential". This	• The information must not be communicated to unauthorized recipients in any form (i.e. in paper or digital form, or the spoken word, etc.). • All documents must bear a watermark with the category of classification "Confidential" written on every page. A property (metadata field) is used to classify the document as "Confidential".	• The information must not be communicated to unauthorized recipients in any form (i.e. in paper or digital form, or via the spoken word, etc.). • Document: a property (metadata field) is used to classify the document as "Internal". • Photo, video, sound: a property (metadata field)	• The information is communicated by the official ICRC channel for public information. • Document: a property (metadata field) is used to classify the document as "Public". • Photo, video, sound: a metadata is used to classify the asset as "Public".

	Strictly confidential	Confidential	Internal	Public
	property must be checked before using the asset. • If the document must be printed, downloaded or stored on an external device (encrypted on an USB stick or hard drive), it must be kept in a secure place (not accessible or visible to unauthorized persons). In addition, it cannot be accessed through an unsecured internet connection. Digital information must be encrypted. • Email: in the title, the word "STRICTLY CONFIDENTIAL" (in uppercase) is written before the subject of the email. No personal data should be contained in the title of the email. • Email: A disclaimer is added at the end of the email which reminds the recipient that this email contains strictly confidential information and must not be forwarded without the authorization of the sender. • Email: links to strictly confidential documents must be used in place of attachments. *See also* Article 8 on ICRC Rules on Data Protection regarding the rights of data subjects to access their own data.	• Photo, video, sound: a property (metadata field) is used to classify the asset as "Confidential". This property must be checked before using the asset. • If the document must be printed, downloaded or stored on an external device (USB Stick or hard drive), it must be kept in a secure place (not accessible or visible to unauthorized recipients and digital information must be encrypted). • Email: in the title, the word "CONFIDENTIAL" (in uppercase) is written before the subject of the email. No personal data should be contained in the title of the email. • Email: A disclaimer is added at the end of the email which reminds the recipient that this email contains confidential information and must not be forwarded without the authorization of the sender. • Email: links to confidential documents must be used in place of attachments. *See also* Article 8 on ICRC Rules on Data Protection regarding the rights of data subjects to access their own data.	is used to classify the asset as "Internal". This property must be checked before using the asset.	