unicef | for every child

ICT Policy Manual

United Nations Children's Fund (UNICEF)
Information & Communication Technology Division

NYHQ, October 2021

Foreword

UNICEF has embraced Information and Communication Technology (ICT) as an enabler to the delivery of its strategic plan. ICT is growing very fast and making significant contributions to UNICEF's achievement.

UNICEF ICT: The mission of UNICEF's ICT Division is to "transform and build partnerships with our stakeholders to successfully implement UNICEF programmers globally through the use of innovative, technology-enabled solutions for better outcomes for children". To achieve this mission, UNICEF ICT abides by three main pillars: Operational Effectiveness, Programme Effectiveness and the Innovative use of Technology.

Undoubtedly, today, UNICEF's workforce is characterized by an increased use and familiarity with ICT solutions to perform their day-to-day work. Besides, the UNICEF workplace is continuously being defined by increasing flexibility and mobility, where employees are able to work however, wherever and whenever they choose.

But all the developments that ICTs bring do not come without risks. The inefficient and/or improper use of ICTs bring about negative impacts to the organization's mission and goals. Various technological measures may be implemented to address the risks. However, these measures are never enough, hence, the need for an ICT policy. Effective ICT policy allows the organization to define how and for what purposes ICTs will be used, while also providing the opportunity to educate employees about ICTs and the risks and rewards associated with them.

ICT Policy Management: The ICT Division, along with key stakeholders, have provided their technical expertise to develop and publish the regulatory documents that are published in the Enterprise Regulatory Framework Library (RF Library) and summarized in this comprehensive ICT policy manual. Presented is a list of issued regulatory documents as well as guidelines for development, classification, naming, numbering and maintenance of these documents.

The purpose of this ICT Policy Manual is to provide an overview of issued ICT regulatory documents (Policy, Standard, Guidance and Procedure) to help ICT managers, ICT staff, and UNICEF personnel at large become familiar of ICT policies and the responsibilities in implementing and applying these policies in their day-to-day work.

I appreciate the effort and professionalism that has been put in the creation of this policy manual and I am sure you will find this a useful tool.

Daniel Couture

Chief Information Officer, UNICEF

Contents

1. INTRODUCTION

ENTERPRISE REGULATORY FRAMEWORK AND THE RF LIBRARY: The UNICEF Regulatory Framework seeks to support risk-informed decision-making and empower staff to ethically, effectively and efficiently undertake their responsibilities by providing up to date policy, procedure, standards and guidance. All approved ICT Regulatory Contents presented in this ICT Policy Manual are published in the Enterprise Regulatory Framework (RF Library).

ICT REGULATORY CONTENTS: UNICEF is a leading humanitarian and development agency working globally for the rights of every child. To achieve this, UNICEF employs Information Communication Technologies (ICT) in vast areas of its global operation to deliver efficient and effective assistance to the beneficiaries. ICT Regulatory Contents (policies, procedures, standards, guidelines, etc.) are the strategic links between UNICEF's mission and its day-to-day operations. The need to have ICT regulatory contents is vital to the smooth and consistent use and operation of technology enabled functions in the entire organization. Accordingly, the ICT Function has developed and implemented various ICT regulatory documents to provide clarity to users when dealing with accountability/responsibility issues or activities that are of critical importance to UNICEF. All UNICEF personnel are expected to comply with the ICT policies, procedures, and standards and follow the guidance provided through the RF Library.

GOAL/PURPOSE OF THIS 'ICT POLICY MANUAL': The purpose of this ICT Policy Manual is to provide an overview of issued ICT regulatory documents (Policy, Standard, Guidance and Procedure) to help ICT managers, ICT staff, and UNICEF staff members at large become aware of ICT policies and their responsibilities in implementing and applying these policies in their day-to-day work.

APPLICABILITY: This ICT Policy Manual applies to all UNICEF personnel and offices.

CONTENT: This manual lays out the ICT regulatory content development tools, process, definitions of the types of regulatory documents issued by UNICEF's ICT Function. It also states the issued policies categorized by topic areas (ICT Business Engagement Management, ICT Solutions Management, ICT Platform and Service Management, ICT Risk Management and Information Management) with a description of the purpose and content of each document. Finally, this manual provides summary of a complete listing of published ICT regulatory documents by title, numbering and type.

2. ICT REGULATORY CONTENT DEVELOPMENT PROCESS

ICT Regulatory documents in the UNICEF ICT function are developed and managed through a lifecycle approach with four key stages: (i) identification of the issue/risk; (ii) regulatory content development; (iii) communication and (iv) regulatory content maintenance. All ICT regulatory content shall be housed in the Enterprise Regulatory Framework platform, an electronic database of policies, procedures, standards, and guidelines that shall be accessible to all UNICEF staff.

2.1 Identification of Issue/Risk

The need for new regulatory content is identified through Organizational entities processes, including, but not limited to the ICT Board, the Global ICT Management Team, Executive decision, GMT recommendation, audit recommendation, evaluation finding, analysis of risk management exceptions/deviations, feedback from users, etc. The Responsible Manager is designated to explore the potential need for new/revised regulatory content. The Responsible Manager consults with the appropriate stakeholders to ensure that (i) the proposed regulatory issue is not already covered under existing regulatory documents and that (ii) new regulatory content would benefit the work of UNICEF Offices without creating unreasonable demands. The Responsible Manager communicates to the ICTD Policy Management the decision to create or change regulatory content. This proposal enables the ICTD Policy Management to more effectively anticipate and plan for the agenda of the Business owners' consultative and appropriate stakeholders.

2.2 Regulatory Content Acceptance Criteria

Any of the following criteria may provide an overwhelming reason to accept or reject a specific suggestion: Purpose; Audience, Authority, Validity, Scope, Uniqueness, Organizational impact and Urgency.

2.3 ICT Regulatory Content Development

The Chief Information Officer (CIO) approves creation/change of ICT Regulatory Content, designates the Responsible Manager who is in charge of coordinating the development and maintenance of the regulatory content. Policies and Rules are issued by the Executive Director. Procedures and Standards are approved and issued by the CIO. Guidance notes can be developed by the ICT Section or Regional and Country levels in consultation with key stakeholders. Guidance is to be approved after consulting the CIO. In each case, the Responsible Manager researches the requirements for the new regulatory content which may include reviewing existing policies, obtaining industry standards and best practices, and conducting interviews with stakeholders affected by the new regulatory content. A draft regulatory content document is created by the Responsible Manager and processed via the ICT Policy Development Tool until it is approved by the CIO or his designate and posted on the Enterprise Regulatory Framework Library and communicated to the target audiences. For more detailed steps on the document development process, see Annex I.

2.4 Regulatory Content Maintenance

The process of amending existing ICT regulatory content is the same as the process of creating and authorizing a new regulatory content. When there are minor changes that do not materially affect the nature of the policy, the task will be assigned to the designated Responsible Document Manager for updating and finally approved by the CIO through the ICT Policy Development process, see Annex I.

Procedure documents may be supplemented periodically with an appendix containing document specific, time bound instructions required for the implementation of a procedure. Appendices from part of the procedure, are mandatory and are only called for the defined timeframe. The Responsible Document Manager is alerted that an ICT regulatory document has reached its mandatory review date or that a revision is required/requested. The Responsible Document Manager consults with key stakeholders and the ICTD Policy Management will facilitate the review by Management group and the RF policy Focal Points as appropriate. If changes to the document are minor, the Responsible Document Manager with the support of the ICT Policy Management updates the Document Management Information page accordingly and the document is posted and communicated. If changes to the document are substantial, the Responsible Document Manager revises the regulatory content and has the document reissued.

If the regulatory content is no longer needed, the Responsible Document Manager requests the ICT Policy Management to retire the document with a note explaining the reason for its retirement, and it is archived for future reference.

3. REGULATORY DOCUMENT CATEGORISATION

UNICEF ICT Function Regulatory documents can be categorized into the following document types:

- **POLICY:** The articulation of an organizational position by the Chief Information Officer (CIO). ICT Policy directs the implementation of the ICT Function's mission, vision, and strategy, in-line with the UNICEF Regulatory Framework. It is defined in high level terms and compliance is mandatory. One or more Procedure and/or Standard documents may be developed to guide the implementation of an ICT Policy.

- **STANDARD:** A set of prescribed principles, processes and/or service level requirements with which all recipients are expected to comply. Deviation from set standards usually will require justification within the accountability framework unless an established exception procedure is followed.

- **GUIDANCE:** Also referred to as “Guidelines”, Guidance notes are developed to facilitate the implementation of the policies, rules, procedures and standards in the UNICEF Regulatory Framework. They are approved and issued by the relevant Business Owner/Division Director. Guidance and/or standard operating procedures may also be issued at the local level for exclusive application in the local management context. Regional Chiefs of ICT may also issue guidance for their respective regions. Guidance notes are not mandatory.
- **PROCEDURE**: A Procedure is a document that provides direction on how to implement the ICT policies in UNICEF. It details how an instituted ICT policy is implemented and sets the parameters of the implementation. Procedures are issued by the CIO or relevant ICT Functional Chiefs known as the Business Owner. Compliance is mandatory.

4. GENERAL STRUCTURE OF ICT REGULATORY DOCUMENTS

- **Rationale:** provides a brief explanation of WHY this policy is required, including for example, decisions mandated by the UN SC/GA or the UNICEF Executive Board.
- **Scope/Applicability:** Indicates if the document is universally applied, or the specific conditions and circumstances for application/implementation (e.g. only applicable to HQ Offices, or only applicable to staff not consultants; etc.)
- **Policy Statements:** elaborate WHAT the policy aims to achieve by using high level statements that clearly and concisely define the issue being addressed, describe the principles that govern the issue and set the parameters and scope for how the issue will be treated within UNICEF.

5. NAMING AND NUMBERING SYSTEM

The following standard nomenclature and numbering system for UNICEF Regulatory Instruments is established:

- **Policies and Rules**: ICEF/POLICY/FUNCTION/YEAR/NUMBER indicating it is an organizational Policy, the functional area it governs, the year it was issued, and the sequential number assigned (e.g.: 001, 002). Revisions of the Policy are tracked by date (e.g.: ICEF/POLICY/FINANCE/2016 /001 v. 3 March 2016).
- **Procedures and Standards**: HEADQUARTERS DIVISION/PROCEDURE/YEAR/NUMBER where the Business Owner is identified by its acronym, the year the Procedure was issued, and the sequential number assigned (e.g.: 001, 002). Revisions of the Procedure are tracked by date (e.g.: DFAM/PROCEDURE/2016/001 v. 3 March 2016).
- **Guidance Notes/Guidelines**: HEADQUARTERS DIVISION/GUIDANCE/YEAR/NUMBER where the Business Owner is identified by the division’s acronym, the year the Guidance was issued, and the sequential number assigned (e.g.: 001, 002). Revisions of the Guidance are tracked by date (e.g.: DFAM/GUIDANCE/2016/001 v. 3 March 2016).

For further information please refer to the UNICEF Procedure on the Regulatory Framework.

6. TOPICS COVERED BY ICT REGULATORY DOCUMENTS

ICT Business Engagement Management

- ❖ **Business Relationship Management (BRM):** Documents that define and support inter-business activities related to aligning business interests with IT deliverables. The documents may consist of procedures, skills and behaviors that foster a productive relationship between UNICEF’s ICT function and the organization’s business partners.
- ❖ **Project Portfolio Management (PPM):** The purpose of PPM is to prioritize, plan and manage projects portfolio efficiently. Regulatory documents in this section include project management capabilities from project inception to approval and then monitor the progress of product development programs and project governance.

- **Governance:** ICT governance defines the lines of authority, accountability and teamwork among the various bodies and units that, together, manage ICT at UNICEF. Documents can describe governance of the system by which ICT is directed and controlled.

ICT Solutions Management

- **Software Development Lifecycle Management:** Process of managing the planning, creation, testing, and deployment of an information system. Documents in this section lay out the accountability framework to encourage desirable behavior in the use of ICT.
- **IT Systems and Data Asset Management:** Documents in this category may include set of business practices that combine inventory, financial and contractual functions to optimize spending and support entire lifecycle (design, construction, commissioning, operating, maintaining, repairing, modifying, replacing and decommissioning/disposal) management and strategic decision-making within the IT environment. Data asset management conserves, curates and exploits valuable enterprise data assets along with their associated Services.

ICT Platform and Service Management

- **Service Delivery and Support:** IT Service Delivery is the process through which an organization provides information technology access to users throughout an application's lifecycle. Service delivery and Support covers the development, deployment, operation and retirement of the IT service. Regulatory documents on the topic also enforce preferred and prohibited approaches to deliver IT services in accordance with regulations or preferred best practices.
- **Identity & Access Management:** Identity and Access Management is a framework for organizational processes that facilitates the management of digital identities and control user access to critical information within UNICEF. Regulatory documents in this section cover organizational policies for managing these digital identities. Documents that discuss the technologies needed to support identity management would also fall into this category.
- **ICT Resource Management:** These documents are related to the efficient and effective development of UNICEF's ICT resources which include tangible resources such as computer hardware or software. Documents related to resource management cover the entire lifecycle, from acquisition, classification, certification, usage to disposal of these resources.
- **Platform and Hosting Management:** Platform Management ensures that appropriate measures are taken to monitor and update IT systems. Hosting Management refers to managing hosted service providers who own or oversees infrastructure or software that is used by UNICEF staff such as cloud services.
- **Network Management:** These documents refer to the process, methods and procedures of administering, operating, managing and provisioning computer networks. It may include a wide range of activities from ensuring proper security performance and reliability of computer networks.

ICT Risk Management

- **Information Security:** Information security refers to a set of strategies to manage the processes, tools and regulatory documents necessary to prevent, detect, document and counter threats to both digital and non-digital information. These documents establish a set of organizational process and standard that aim to protect UNICEF's information assets.
- **BCP/DR, Emergency Preparedness & Support:** Emergency Preparedness refers to the processes of planning, organizing, evaluating and acting in an effort to ensure effective coordination during an emergency situation. Documents in this section cover policies on disaster recovery and emergency preparedness, telecommunications and support.
- **ICT Regulatory Management and Audit:** Regulatory Management refers to developing and managing regulatory documents (Policies, Standards, Procedures and Guidance) to ensure regulatory compliance. Documents in this section help ensure that UNICEF's core business

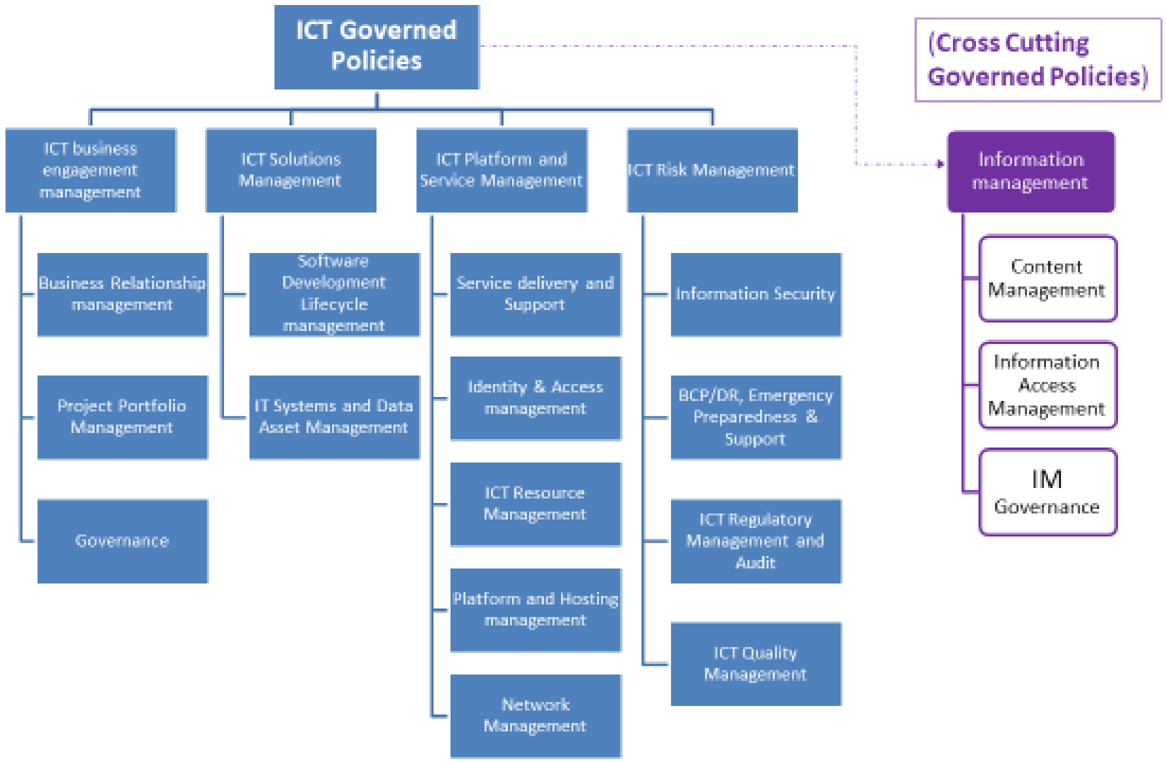
does not violate relevant regulations, in the jurisdiction in which the business is situated, governing the sectors where the enterprise operates.

- **ICT Quality Management:** Documents may focus on meeting customer requirements and enhancing their satisfaction in line with the four main components: quality planning, quality assurance, quality control and quality improvement. It should align with UNICEF's purpose and strategic direction as expressed in the organizational goals, policies, processes and resources needed to implement and maintain it.

Information Management

- **Content Management:** Content Management is the process for collection, delivery, retrieval and overall management of information in all formats. Regulatory documents in this section covers the administration of the digital lifecycle.
- **Information Access Management:** Access Management is the process of identifying, controlling and managing authorized users' access to an IT system/application and data/documents.
- **IM Governance:** Governance provides content creators with structure and guidelines. Documents in this section ensure appropriate behavior in the creation, storage, use, archiving and deletion of information. It includes standards, processes, responsibilities and policies that ensure the effective and efficient use of information in enabling UNICEF to achieve its mission.

UNICEF ICT Policy Framework


ICT Governed Policies
(Cross Cutting Governed Policies)
ICT business engagement management
ICT Solutions Management
ICT Platform and Service Management
ICT Risk Management
Information management
Business Relationship management
Project Portfolio Management
Governance
Software Development Lifecycle management
IT Systems and Data Asset Management
Service delivery and Support
Identity & Access management
ICT Resource Management
Platform and Hosting management
Network Management
Information Security
BCP/DR, Emergency Preparedness & Support
ICT Regulatory Management and Audit
ICT Quality Management
Content Management
Information Access Management
IM Governance

7. LIST OF ISSUED POLICIES

	Category	Title	Reference Number	Type	Translated
ICT BUSINESS ENGAGEMENT MANAGEMENT	Project Portfolio Management	UNICEF Policy on ICT Project Management and Governance	POLICY/ICTD/2020/001	POLICY	Spanish French
		UNICEF Procedure on Project Portfolio Management and Governance	PROCEDURE/ICTD/2020/001	PROCEDURE	Spanish French
	Governance	UNICEF Guidance for ICT Management in UNICEF Offices	GUIDANCE /ICTD/2020/001	GUIDANCE	Spanish French
ICT SOLUTI ONS	Software Development Lifecycle Management	UNICEF Standard on Software Acquisition and Management	ICTD/STANDARD/2019/003	STANDARD	
ICT PLATFORM AND SERVICE MANAGEMENT	Service Delivery and Support	UNICEF Standard on IT Service Management (ITSM)	STANDARD /2019-001	STANDARD	
		UNICEF Standard on Cloud based email and related Office 365 services	STANDARD /2015-001	STANDARD	
		UNICEF Guidance on Incident Management for National Committees and Partners of UNICEF Branded Web Sites	GUIDELINE /2009-003	GUIDANCE	
		UNICEF Procedure on ITSM Release and Deployment Management	PROCEDURE /2012-002	PROCEDURE	
		UNICEF Procedure on ITSM Problem Management	PROCEDURE /2012-003	PROCEDURE	
		UNICEF Procedure on ITSM Incident Management	PROCEDURE /2012-004	PROCEDURE	
		UNICEF Procedure on ITSM Change Management	PROCEDURE /2012-005	PROCEDURE	
		UNICEF Procedure on Release Management for Office 365 Services	PROCEDURE /2016/003	PROCEDURE	
		UNICEF Procedure on NYHQ Conference Services - SOP		PROCEDURE	
	Identity & Access Management	UNICEF Procedure on Granting, Modifying and Revoking User Access to ICT Resources	PROCEDURE /2012-001	PROCEDURE	
	ICT Resource Management	UNICEF Policy on the Use of Mobile Devices	POLICY /2013-003 Rev. 01 March 2017	POLICY	Spanish French
		UNICEF Standard on Computer Hardware	STANDARD /2018/011	STANDARD	Spanish French
		UNICEF Guidance on the Use of Mobile Devices	GUIDELINE /2013-001 Rev 01 March 2017	GUIDANCE	Spanish French
		UNICEF Guidance for Standardization of the Assistive Technology (AT) Products		GUIDANCE	

		UNICEF Procedure on Computer Disposal	PROCEDURE /2017/001	PROCEDURE	Spanish French
	Platform and Hosting Management	UNICEF Guidance on Public Cloud Services Provisioning	GUIDANCE /2016/008	GUIDANCE	
		UNICEF Procedure on Physical Access to NYHQ Data Centers	PROCEDURE /2016/004	PROCEDURE	
	Network Management	UNICEF Standard on Network Naming and Hardware Equipment	STANDARD /2017/001	STANDARD	
		UNICEF Guidance on ICT Connectivity Bandwidth Planning for Field Offices	GUIDELINE/ 2015-002 Rev. 27 November 2017	GUIDANCE	Spanish French
		UNICEF Guidance on LAN-WiFi	GUIDANCE /2017/001	GUIDANCE	
ICT RISK MANAGEMENT	**Information Security**	UNICEF Policy on Information Security	POLICY /2014-001	POLICY	Spanish French
		UNICEF Standard on Information Security: Asset Management	STANDARD /2018/001	STANDARD	Spanish French
		UNICEF Standard on Information Security: Access Control	STANDARD /2018/002	STANDARD	Spanish French
		UNICEF Standard on Information Security: ICT Operations Security	STANDARD /2018/003	STANDARD	
		UNICEF Standard on ICT Network Communications Security	STANDARD /2018/004	STANDARD	
		UNICEF Standard on information Security: Incident Management	STANDARD /2018/005	STANDARD	Spanish French
		UNICEF Standard on Information Security: Physical and Environmental Security	STANDARD /2018/006	STANDARD	
		UNICEF Standard on Information Security: ICT Systems Acquisition, Development and Maintenance	STANDARD /2018/007	STANDARD	
		UNICEF Standard on Information Security: Cryptography	STANDARD /2018/008	STANDARD	
		UNICEF Standard on Information Security: Vendor Management	STANDARD /2018/009	STANDARD	
		UNICEF Standard on Acceptable Use of ICT Resources	STANDARD /2018/010	STANDARD	Spanish French
		UNICEF Data and Information Classification and System Controls Reference	Version 1.2 Dec 2017	REFERENCE DOCUMENT	
		UNICEF Policy on Website Information Security	POLICY /2012-009	POLICY	

		UNICEF Standard on Exception to Website Information Security Policy Minimum Control	STANDARD /2015/002	STANDARD	
	BCP/DR, Emergency Preparedness & Support	UNICEF Guidance on ICT Disaster Recovery for Field Offices	GUIDANCE/2015/001 Rev 15 August 2017	GUIDANCE	
		Emergency Telecommunications Handbook		STANDAD & GUIDANCE	
	ICT Regulatory Management and Audit	UNICEF Procedure on the Regulatory Framework	DFAM Policy 1 Supplement 4	PROCEDURE	
INFORMATION MANAGEMENT	**Content Management**	UNICEF Standard on Public Facing Website Hosting	STANDARD /2019-001	STANDARD	
		UNICEF Guidance on How to Produce Accessible Content		GUIDANCE	
	Information Access Management	See: UNICEF Standard on Information Security: Access Control	STANDARD /2018/002	STANDARD	Spanish French
		UNICEF Procedure on User Access to the UNICEF Archives	DFAM/PROCEDURE /2019/007	PROCEDURE	Spanish French
	IM Governance	UNICEF Standard on Conversion of Images into Text-Searchable Documents	STANDARD /2018/012	STANDARD	
		UNICEF Guidance on Digitization of Archival Materials	GUIDANCE /2018/001	GUIDANCE	Spanish French
		UNICEF Guidance on Scanning of Business Documents	GUIDANCE /2018/002	GUIDANCE	Spanish French
		UNICEF Procedure on Information Management	ICTD/PROCEDURE/ 2019/001	PROCEDURE	Spanish French
		UNICEF Procedure on Destruction of Electronic Records	ICTD/PROCEDURE/ 2019/002	PROCEDURE	Spanish French
		UNICEF Procedure on Destruction of Physical Records	DFAM/PROCEDURE /2019/002	PROCEDURE	Spanish French
		UNICEF Procedure on Retention of Recorded Information	DFAM/PROCEDURE /2019/003	PROCEDURE	Spanish French
		UNICEF Procedure on Archival Material with Restricted Access	DFAM/PROCEDURE /2019/004	PROCEDURE	Spanish French
		UNICEF Procedure on Sending Documents to Offsite Storage	DFAM/PROCEDURE /2019/005	PROCEDURE	Spanish French
		UNICEF Standard on Archival Description	DFAM/STANDARD/2019/006	STANDARD	Spanish French
		UNICEF Procedure on Transferring Materials to UNICEF Archives	DFAM/PROCEDURE /2019/010	PROCEDURE	
		UNICEF Guidance on Handling of Physical Archival Materials	DFAM/GUIDANCE/2019/001	GUIDANCE	
		UNICEF Procedure on Archival Acquisition and Accessioning	DFAM/PROCEDURE /2019/011	PROCEDURE	

		UNICEF Guidance on Management of Archival Collections	DFAM/GUIDANCE/2019/002	GUIDANCE	

8. ISSUED REGULATORY DOCUMENTS

8.1. ICT Business Engagement Management

*8.1.1. **Business Relationship Management***

BRM related regulatory documents will be added to this section.

*8.1.2. **Project Portfolio Management***

UNICEF Policy on ICT Project Management and Governance

The purpose of this policy is to establish a uniform project management framework and lay out the requirements and methodology for managing and recording UNICEF ICT-enabled projects to promote consistency, quality and accountability; thereby reducing risks and increasing project success. The policy addresses the organizational need to achieve optimal outcomes of investments, while ensuring effective management of resources.

This policy discusses best practices in governance of organizational ICTs using project management methodology based on the Project Management Institute (PMI) framework and selected processes from PRINCE2. Exceptions, accountabilities for implementation and responsibilities are also considered in the document.

UNICEF Procedure on Project Portfolio Management and Governance

The purpose of this procedure is to inform staff and stakeholders of the procedure for planning, developing, deploying and managing UNICEF Information and Communication Technology (ICT)-enabled proposals and projects within the UNICEF Project Portfolio Management (PPM) framework. The procedure establishes a system of record and process for prioritizing demand, assisting management in making informed decisions on what ICT investments are most viable and strategic in the context of constrained resources. This procedure applies to all UNICEF project/Business owners or sponsors who initiate ICT-enabled projects. Such projects typically involve software application development, software configurations or software subscription services, and/or technical architecture, security, networking and engineering solutions. The procedure applies to all personnel that are assigned ICT project management/support responsibilities.

This procedure discusses portfolio cycles, process of approval of funding and on-going reviews, demand management (registration, classification and ICT review), project management methodologies and special considerations in emergency contexts. Responsibilities of key stakeholders are also laid out in the procedure.

*8.1.3. **Governance***

UNICEF Guidance for ICT Management in UNICEF Offices

The purpose of this guidance is to assist UNICEF Country, Regional, and HQ Offices to plan and budget for the ICT requirements. The guidance applies to all UNICEF offices globally.

This guidance discusses local ICT Governance and oversight, human resources, capacity management and learning, standard ICT infrastructure and connectivity, standard hardware and equipment, standard software and licenses. It also mentions emergency preparedness, security communications and business continuity, UN coherence and harmonization efforts. It also includes recommended field structure for IT and telecoms.

8.2. ICT Solutions Management

8.2.1. Software Development Lifecycle Management

UNICEF Standard on Software Acquisition and Management (ICTD/STANDARD/2019/003)

This standard establishes the principles for software acquisition, compliance and governance for all types of software assets acquired and/or subscribed to/by UNICEF. Through this standard, UNICEF effectively manages and controls its procured assets, with a view, among others, to comply with legal requirements, enhance effective and efficient use of software assets and minimize the risk to organizational information and information systems.

This standard is not applicable to acquiring application solutions via development or software configuration services. Refer to Project Portfolio Management and Governance Policy/Procedure for Software/application solution development or software configuration solutions.

8.2.2.IT Systems and Data Asset Management

IT Systems and Data Asset Management related regulatory documents will be added to this section.

8.3. ICT Platform and Service Management

8.3.1. Service Delivery and Support

UNICEF Standard on IT Service Management (ICTD/STANDARD/2019/001)

This Standard ensures that ICT Services are aligned with UNICEF business needs and objectives, continually improve the utilization of resources, the quality of project deliverables and timescales, risk management and resilience, and user satisfaction.

This standard applies to all ICT Functions in UNICEF globally. The following IT Service Management process and functions are in the scope: Service Desk, Service Catalogue, Incident Management, Problem Management, Release & Deployment Management, Change Management, Knowledge Management, Service Level Management, and Continual Service Improvement.

UNICEF Standard on Cloud-based email and related Office 365 services (CF/ITSS/STANDARD/2015-001)

The purpose of this standard is to is to provide a reference of the operational standards for cloud-based email and related Office365 services (services (MS-Exchange, MS-Outlook, Skype for Business, and OneDrive for Business) provisioning and support and prioritize the standardization of the UNICEF messaging environment and related cloud services. The standards are to support ICT teams, Subject Matter Experts (SMEs), Local Site Administrators (LSAs), and UNICEF end-users.

This standard discusses service availability, access to email and related Office365 services, service offering and features, languages, software, data storage and quotas, data-recovery (available to end-users), security, bulk email, identity information of users in Global address list, OneDrive synchronization, technical support as well as maintenance periods and outage periods. The standard also covers email online archiving, email distribution groups, shared mailboxes, rooms and resources, generic accounts, naming convention and standards names, user account provisioning, users moving to another duty station, users leaving and returning to the organization. Finally, the document also mentions special considerations in emergency contexts and responsibilities.

UNICEF Guidance on Incident Management for National Committees and Partners of UNICEF-Branded Web Sites (CF/ITSS/GUIDELINE/2009-003)

The purpose of this guidance is to assist National Committees on the appropriate response to, and management of incidents via the web. National Committee web sites and other partner web sites that host UNICEF artifacts, logos and other branding information need to maintain a high degree of vigilance to identify, manage and contain any security incidents. All non-UNICEF websites that have entered into agreements to host any UNICEF content or utilize any UNICEF brand items such as logos, official documents and others must adhere to this guideline.

The guidance discusses identification of incidents, containment strategies, eradication and recovery. It also lays out responsibilities of the National committee (Partner) IT Manager and UNICEF's Chief of IT Security and provides an incident identification form and an incident contact list to fill out and forward to UNICEF's Chief of IT Security for reference.

UNICEF Procedure on ITSM Release and Deployment Management (CF/ITSS/PROCEDURE/2012-002)

The purpose of this Release and Deployment Process Procedure publication is to enforce the ICTD Release and Deployment Management Policy throughout the organization and serve as guidance for ICT staff involved on service design, implementation and support, while integrating teams and maintaining clear lines of accountabilities and responsibilities. This publication sets formal Release and Deployment Management Process procedures, both technical and non-technical, to be followed by all stakeholders at field and headquarter offices.

This procedure discusses the steps that must be carried out to support the enforcement of Release and Deployment Management Policy.

UNICEF Procedure on ITSM Problem Management (CF/ITSS/PROCEDURE/2012-003)

The purpose of this procedure is to set the overall ICT Problem Management process and procedure for the UNICEF ICT infrastructure and environment. Problem Management at UNICEF manages the lifecycle of all problems related to ICT infrastructure and services with the primary goal of proactively preventing incidents from occurring and minimizing the impact of active incidents through root cause analysis, solutions and workarounds. The scope of the Problem Management process at UNICEF includes the activities, IT Service Management (ITSM) tools, ICT functions and roles needed to diagnose the root cause of incidents and to determine the resolution to those problems.

This procedure discusses UNICEF's approach to Problem Management, the objectives of the process and lays out the Problem Management process and procedures (Process Ownership, Integration, Flow), problem detection, logging and categorization, prioritization and planning, investigation and diagnosis, known error logging and investigation, as well as governance and reporting.

UNICEF Procedure on ITSM Incident Management (CF/ITSS/PROCEDURE/2012-004)

The purpose of this procedure is to set the overall ICT Incident Management process and procedure for the UNICEF ICT infrastructure and environment. The Incident Management process at UNICEF manages the lifecycle of all incidents affecting the ICT infrastructure and services with the primary goal of restoring service to users as quickly as possible. The procedure took the existing Incident Management practices and ICT best practices as input. The Country and/or Regional ICT Chiefs will provide any guidance about any additional procedures that may be needed specific to the offices.

This procedure discusses the activities, IT Service Management (ITSM) tools, ICT functions and roles needed to identify, log, troubleshoot and resolve incidents in order to restore service to normal operations, according to agreed service levels of the Incident Management process. It also outlines all the steps of incident management from identification to resolution, roles and responsibilities of the stakeholders of incident resolution and management processes, escalation mechanism, major incident management, incident management governance, incident reporting and Key Performance indicators.

UNICEF Procedure on ITSM Change Management (CF/ITSS/PROCEDURE/2012-005)

The purpose of this document is to describe the UNICEF Change Management Process. In addition to identifying Change Management roles, sub-processes and activities, this document also includes policies to guide the adoption and enforcement of the overall Change Management process.

This procedure discusses the different stages of the Change Management process and procedures, including integration, logging, review, assessment and planning, approval, implementation, evaluation and change closure, governance and reporting.

UNICEF Procedure on Release Management for Office 365 Services (CF/ITSS/PROCEDURE/2016/003)

The purpose of this procedure is to introduce the way Office 365 features and services are released to UNICEF users. The creation of this document came in the course of C4 programme, as a need to adapt ICTD practices for release and deployment of changes and/or new services to the specifics of O365 release practices applied by Microsoft. This procedure applies to Office 365 services only and it is intended for use by O365 Service Owner, Operations and Supporting teams as well as ICT Staff at field, regional and headquarter offices.

This procedure discusses the categorization of release changes for O365 and applicable procedures, required tenants for Office 365 services, required steps in the procedure (monitor, evaluate, configure and release), service ownership and internal controls. The procedure also covers procedure requirements and workflows, responsibilities and important definitions.

UNICEF Procedure on NYHQ Conference Services - SOP

The purpose of this document is to clarify the procedures for requesting event/conferencing services, outlining the resources and support requirements. This Standard Operating Procedure (SOP) will help prevent issues in both NYHQ locations (3 UN Plaza and 633 Third Ave) related to scheduling conflicts to ensure that UNICEF events/conferences/meetings are properly supported.

This procedure discusses a comprehensive list of available conference rooms and services, methods for reserving conference rooms (self-service, teleconferencing, video conference) and support, live streaming, requesting brand signage/visibility materials as well as making additions, changes and cancellations. The standard also discusses follow-up and escalation practices and support for events outside UNICEF House / 633 Third Avenue.

8.3.2. Identity & Access Management

UNICEF Procedure for Granting, Modifying and Revoking User Access to ICT Resources (CF/ITSS/PROCEDURE/2012-001)

The purpose of this procedure is to outline the steps for granting, modifying, and revoking user access to Information & Communication Technology (lCT) resources. It furthers the policy "Access Control for UNICEF's Information Assets". This document defines the procedures necessary to grant and revoke user access to lCT resources globally. It applies to all staff members, individual contractors, consultants, service-providers, and external business partners with access to restricted UNICEF lCT resources. This revision includes changes for access management considerations after the organizational transition to the common global Enterprise Resource Planning system VISION with its various transaction management components.

This procedure discusses granting users access to ICT resources, processes for revoking user access to ICT resources, modifying user access, access for UNICEF partners (special representatives, national committees, staff from other UN agencies hosted in UNICEF premises), reactivating user accounts, keywords and important definitions.

8.3.3. ICT Resource Management

UNICEF Policy on the Use of Mobile Devices (CF/ITSS/POLICY/2013-003 Rev. 01 March 2017)

The purpose of this policy is to outline the usage, user responsibilities, reimbursement policies, remote wipe and device management and level of technical support users can expect for personal devices and UNICEF-issued devices as well as user responsibilities and organizational responsibilities.

This policy discusses UNICEF's responsibility to protect its information assets in order to safeguard its intellectual property and reputation as well as exception and accountabilities for implementation. A guidance document has been drafted to facilitate the implementation of this policy.

UNICEF Standard on Computer Hardware (ICTD/STANDARD/2018/011)

The purpose of this standard is to outline ICT's standards for computer hardware to ensure efficient support by the ICT Function. It is not possible to support hardware from all vendors in a timely manner. It is especially important at UNICEF, where ICT staff must setup, maintain, repair, and support hundreds/thousands of computer devices in each office. In order to get the best value on computer hardware compatible with its infrastructure, UNICEF has set the computer hardware in this standard that can be used by all offices. LTAs shall also be defined for these standards from where offices can place purchase orders directly. The intention of ICTD's issuance of this standard document is not to impose restrictions that are contrary to UNICEF's culture, but instead to underscore our commitment to provide effective ICT systems/services and efficient ICT support. This Computer Hardware standard document applies to all UNICEF offices globally.

This standard discusses standard requirements and workflow, computer hardware standards (desktop, laptop, server, printer, etc.) and types of hardware support and administration. Exceptions, special considerations in emergency contexts and responsibilities are also considered in the document.

UNICEF Guidance on the Use of Mobile Devices (CF/ITSS/GUIDELINE/2013-001 Rev 01 March 2017)

The purpose of this guidance is to establish standard and best practice guidance for the use and management of mobile devices which are accessing UNICEF's IT resources. The goal is to ensure that mobile device current standards, security requirements and best practices are easily understood and adhered to by all parties. This guidance will facilitate implementation of the UNICEF Policy on the use of Mobile Devices (CF/ITSS/POLICY/2013-003 Rev. 01 March 2017). This guidance applies to all mobile device users accessing UNICEF IT resources. It also applies to all forms of mobile devices including, but not limited to mobile phones and tablets.

This guidance discusses the current best practices for the use of mobile devices, notably, eligible devices and platforms, mobile applications, security guidelines and best practices for all mobile devices.

UNICEF Guidance for Standardization of Assistive Technology (AT) Products

The purpose of the guidance is to ensure UNICEF stakeholders, including employees, have an accessible workplace. UNICEF ICTD is committed to inclusion for all stakeholders and has created this guidance to focus on Accessibility, Inclusion and Support for ICT products and services and particularly the standardization of assistive technology products.

This guidance discusses the definition of assistive technology and includes a list of assistive technologies by disability, descriptions of assistive technology products as well as evaluation criteria for the procurement of assistive technology.

UNICEF Procedure on Computer Disposal (ICTD/PROCEDURE/2017/001)

The purpose of this procedure is to provide disposal requirements for protecting UNICEF's ICT assets by either of two methods: (1) destruction of the ICT device; or, (2) complete removal of all electronic data from the computer storage device. This procedure applies to all UNICEF offices: headquarters locations, country offices, and regional offices. It covers all computers, other computing devices, and accessory equipment that store electronic data, information, and software programs. The main objective of this procedure is to safeguard the confidentiality, potential misuse/abuse of UNICEF's information and data.

This procedure discusses disposal requirements, suggested data removal utility and method, the three-pass method, satellite equipment disposal, network equipment disposal, two-way radio and mobile satellite communications disposal and mobile phone disposal. The document also mentions special considerations in emergency contexts and responsibilities.

8.3.4. Platform and Hosting Management

UNICEF Guidance on Public Cloud Services Provisioning (CF/ICTD/GUIDANCE/2016/008)

The purpose of this guidance is to provide a comprehensive overview of the process through which UNICEF will be, subscribing, commissioning resources and tracking resource utilization and expenditures as part of the current arrangements with our Cloud Providers. This process includes elements such as defining eligibility to access cloud services, expectations in terms of architectural draft, planning and budgeting for Services, purchasing/subscribing to services, payment and monitoring and the request and authorization process.

This guidance discusses necessary steps in project registration, draft architecture and resource forecast, definition of the operational model, integration with other UNICEF applications and services, financial commitment, platform positioning and creation of the deployment environment, ongoing financial controls and follow-up financial commitments. The document also includes responsibilities and a chart for project initiation including cloud provisioning and the ordering process.

The scope of this document is limited to the provisioning process and basic governance in relation to the accounts, subscriptions and deployments on the Cloud Providers. This document does not cover aspects related to the design (including integration or security), Quality Assurance, or the Operationalization of solutions based on these cloud services.

UNICEF Procedure on Physical Access to NYHQ Data Centers (ICTD/PROCEDURE/2016/004)

The purpose of this procedure is to define the physical access process, list authorized personnel and access procedures to UNICEF NYHQ Data Centers. This procedure applies to both UNICEF NYHQ Data Centers at 3 UN Plaza, SunGard as well as 633TA equipment room.

This procedure discusses the steps required to access 3 UN Data Centre, SunGard and the 633TA Equipment area with and without cardkey access. It also defines special considerations in emergency contexts and responsibilities.

8.3.5. Network Management

UNICEF Standard on Network Naming and Hardware Equipment (ICTD/STANDARD/2017/001)

The purpose of this standard is to define UNICEF Network Naming convention, LAN ID, Network Hardware Equipment to be used for architecting and delivering and supporting LANs in UNICEF Field Offices. This Standard applies to all UNICEF Field Offices and ICT Officers engaged in the implementation and maintenance of UNICEF Network.

This standard discusses naming conventions for network nodes, labelling recommendations, managing IP subnet addressing space in a LAN, VLAN IDs, network equipment standards, core switches/routers, universal WiFi modules and responsibilities.

UNICEF Guidance on ICT Connectivity Bandwidth Planning for Field Offices (CF/ITSS/GUIDELINE/2015-002 Rev. 27 November 2017)

The purpose of this guidance is to establish a Minimum Bandwidth for Business (MBB) for UNICEF offices, which is the minimum quantity of network bandwidth that an office is recommended to have to ensure that an acceptable user experience can be offered to all office staff when using UNICEF corporate systems. This guidance applies to all UNICEF offices, except Budapest and the HQ offices in New York, Geneva and Copenhagen.

This guidance discusses the availability of an Online Calculator indicating the Minimum Bandwidth for Business (MBB) that offices need to utilize UNICEF business systems in a productive and effective manner. It also mentions data points for cost estimations.

UNICEF Guidance on LAN-WiFi (ICTD/GUIDANCE/2017/001)

The purpose of this guidance is to provide guidelines for architecting and delivering LANs in UNICEF Country Offices and Field Offices. This is a normative document covering UNICEF best practices to deliver network-related business critical services: Internet, WAN, DMZ, Video Conference, WiFi, IP Telephony, connectivity to remote offices and/or essential staff residences and Disaster Recovery “hot-standby” sites. It also covers LAN management best practices as well as related operating procedures. This document is for use by all UNICEF ICT staff engaged in LAN design, development and maintenance.

This guidance discusses guiding principles, architecture principles, logical LAN layouts, additional details and optional networking solutions, LAN management and monitoring, IT staff training and standard operating procedures. It provides guidance in global standards and best practices. It was written to provide answers to the following types of questions: how should WiFi or Video Conference be connected in the network, on which firewall port/zone a specific service should be, how should the Disaster Recovery or Remote sites be connected, what should be the logical/physical layout of the LAN, are VLANs needed, etc. This document describes logical and physical “blueprints” of the UNICEF CO/FO LANs. Hardware standards change more frequently and therefore are part of a separate accompanying document.

8.4. ICT Risk Management

8.4.1. Information Security

UNICEF Policy on Information Security (CF/ITSS/POLICY/2014-001)

The purpose of this policy is to establish Executive Management's endorsement of management principles to govern the UNICEF Information Security Program and supporting Information Security policies. This Information Security Program aims at protecting UNICEF Information Assets as well as UNICEF Information and Communication Technologies (ICT) from any threat whether internal or external, deliberate or accidental. The basis of this policy is in accordance with the UN recommended and globally recognized standard ISO 27001 (International Standards Organization).

This policy discusses objectives, expected results, program scope & boundary, information security organization, legal and regulatory requirements, resourcing, approach to enterprise risks and accountabilities for implementation.

UNICEF Standard on Information Security: Asset Management (ICTD/STANDARD/2018/001)

The purpose of this standard is to provide an organizational framework to identify, classify, and establish control requirements for UNICEF information assets. Furthermore, this standard provides a foundational principle for protecting information assets based on its organizational value. This standard applies to all UNICEF staff, contractors, ICT Centers as well as outsourced providers (Cloud, Application Developers or Hosting Facilities).

This standard discusses asset protection, privacy and monitoring, information asset characterization and classification (public, internal and confidential), information asset handling and ownership. Exceptions, special considerations in emergency contexts and responsibilities are also considered in the document.

UNICEF Standard on Information Security: Access Control (ICTD/STANDARD/2018/002)

The purpose of this standard is to reduce risks of human error, theft, fraud, or misuse of UNICEF information assets by granting access rights to these assets solely to users with authorized credentials. Access to UNICEF information systems resources and information will be strictly controlled, monitored, and tracked on the basis of business and security requirements. This domain includes implementation of internal and external access controls across all electronic forms of information processing and communications systems, applications, networks, and mobile platforms. This standard applies to all staff members, contractors, vendors and partners involved in UNICEF service delivery with a UNICEF-owned, vendor-owned, or personally owned computing device used to connect to the UNICEF network, whether onsite or through a remote connection.

This standard discusses the authority and requirements for access approval, access categories (administrative, privileged or default), user registration, unique account identity and password management. It states password complexity requirements, secure logon procedures, user deprovisioning, privilege management and access control mechanisms. Finally, it discusses user responsibilities, access rights, exceptions and special considerations in emergency contexts.

UNICEF Standard on Information Security: ICT Operations Security (ICTD/STANDARD/2018/003)

The purpose of this standard is to establish the operational IT / Information Security requirements pertaining to staff and ICT equipment in accordance with Information Security Programme. This standard applies to all UNICEF staff, contractors, ICT Centers as well as outsourced providers (Cloud, Application Developers or Hosting Facilities).

This standard discusses documented procedures, systems/software change management, change restrictions to software packages, segregation of duties and capacity management. It also touches upon protection from malware, scanning traffic, clock synchronization, control of operational software and hardware. Other topics mentioned include management, transit and disposal of media, logging, data communication monitoring as well as BCP and disaster recovery.

UNICEF Standard on ICT Network Communications Security (ICTD/STANDARD/2018/004)

The purpose of this standard is to provide guidance on safe information transfer mechanisms that address security of information on UNICEF ICT's global network. This standard is to be implemented based on data classification as defined in the UNICEF Data and Information Classification and System Controls Reference. This standard applies to all UNICEF staff, contractors, ICT Centers as well as outsourced providers (Cloud, Application Developers or Hosting Facilities).

This standard discusses network controls, communication channel use, security of network services, information transfer policies and procedures, agreements on information transfer, electronic messaging and confidentiality/nondisclosure agreements or contractual clauses. Exceptions, special considerations in emergency contexts and responsibilities are also considered in this document.

UNICEF Standard on Information Security: Incident Management (ICTD/STANDARD/2018/005)

The purpose of this standard is to outline a consistent and effective approach to the management of information security incidents, including communication on events and weaknesses. The standard shall be implemented by following the methods and guidelines specified in the UNICEF Data and Information Classification and System Controls Reference. This standard applies to all UNICEF ICT staff, contractors, ICT Centers as well as outsourced providers (Cloud, Application Developers or Hosting Facilities).

This standard discusses incident management, responsibilities and procedures, incident detection, monitoring and reporting as well as appropriate responses to information security incidents. The standard also examines security incident initiation thresholds, team membership and notification order as well as steps in the process of evidence collection and responsibilities.

UNICEF Standard on Information Security: Physical and Environmental Security (ICTD/STANDARD/2018/006)

The purpose of this standard is to establish physical and environmental security requirements pertaining to staff and ICT equipment. Specifically, the standard provides further guidance to prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities. This standard applies to all UNICEF ICT staff, contractors, ICT Centers as well as outsourced providers (Cloud, Application Developers or Hosting Facilities).

This standard discusses security controls, physical entry controls, the process for securing offices, rooms and facilities and safeguarding against external and environmental threats. The document also focuses on equipment security, siting and protection, cabling security, equipment maintenance, security of equipment off-premises, removal of assets and appropriate protection for unattended user equipment.

UNICEF Standard on Information Security: ICT Systems Acquisition, Development and Maintenance (ICTD/STANDARD/2018/007)

The purpose of this standard is to ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems that provide services over public networks. The standard also provides requirements to ensure that information security is designed and implemented within the development lifecycle of information systems. Furthermore, it provides guidance on the design and implementation of the information system supporting the business process for security. All such requirements shall be identified, justified, agreed, and documented at the requirements phase of a project. This standard applies to all UNICEF ICT staff, contractors, ICT Centers as well as outsourced providers (Cloud, Application Developers or Hosting Facilities).

This standard discusses service requirements specification, securing application services on public networks, protecting electronic commerce services and transactions, software development regulatory contents, correct processing in applications and management of program source code. The document also focuses on control of operational software (acquisition, development and use of development tools), outsourced software development, developmental testing and protection of system test data. Other topics that are mentioned include change management, change restrictions, controls for mobile code, system configuration, review and acceptance, cloud services, electronic messaging and business information systems.

UNICEF Standard on Information Security: Cryptography (ICTD/STANDARD/2018/008)

The purpose of this standard is to provide guidance for protecting UNICEF information while in use, during its transmission (in transit) and while at rest (stored) in accordance with its organizational value, as noted in both UNICEF Standard on Asset Management, and UNICEF Data and Information Classification and System Controls Reference. This standard applies to all UNICEF ICT staff, contractors, ICT Centers as well as outsourced providers (Cloud, Application Developers or Hosting Facilities).

This standard discusses the cryptographic controls that shall be used to achieve UNICEF's information security objectives and cryptographic systems that can be used to provide cryptographic services. Encryption key management processes are also touched upon to ensure the protection of keys against disclosure, modification, loss or destruction. Exceptions, special considerations in emergency contexts and responsibilities are also considered.

UNICEF Standard on Information Security: Vendor Management (ICTD/STANDARD/2018/009)

The purpose of this standard is to ensure protection of UNICEF's information assets that are accessible by service vendor and maintains an agreed level of security and availability in line with the approved General Terms and Conditions (GTC) verbiage in the vendor agreements. This standard applies to all UNICEF ICT staff, contractors, ICT Centers as well as outsourced providers (Cloud, Application Developers or Hosting Facilities).

This standard discusses the information security requirements for mitigating the risks associated with service vendor's access to UNICEF's information. The document also discusses cloud services management, service level agreements (SLAs) between service providers and UNICEF, information and communication technology services as well as vendor service delivery management. Exceptions, special considerations in emergency contexts and responsibilities are also considered in the document.

UNICEF Standard on Acceptable Use of ICT Resources (ICTD/STANDARD/2018/010)

The purpose of this standard is to complement the UN staff rules and regulations, to establish what is considered "acceptable use" of UNICEF's Information Communication Technology Assets. This standard applies to all UNICEF staff, contractors, ICT resources as well as outsourced providers (Cloud, Application Developers or Hosting Facilities).

This standard discusses limited personal use of UNICEF ICT resources, information and data storage, appropriate use of email, social media and communication activities and copyright and intellectual property laws. The document also focuses on appropriate use of UNICEF equipment/software, privacy and monitoring and non-compliance. Exceptions, special considerations in emergency contexts and responsibilities are also considered in the document.

UNICEF Data and Information Classification and System Controls Reference

The purpose of this reference document is to provide UNICEF Stakeholders (Business Units) and ICTD a central reference that can be used to streamline the Information, System Classification and Inventory process. This document shall be viewed as the authoritative reference detailing UNICEF's Data/Information Classification processes, ICT Systems Classification, Security Control Requirements based on the System Classification and Security Assessment requirements.

This reference document discusses the classification of all systems and devices based on the high-water mark of the information that they store, process and/or transmit. Subsequently the underlying security controls will in-turn be commensurate with the classification of the system. The document covers information classification, system classification, control requirements, user audience, system control requirements and operational impact.

UNICEF Policy on Website Information Security (CF/ITSS/POLICY/2012-009)

The purpose of this policy is to minimize the organizational risks to which UNICEF is exposed through its presence on the web. This policy applies to all UNICEF Websites that are hosted in-house as well as those sites hosted and or supported by third party service providers. This policy supports UNICEF's brand protection, information security efforts, UNICEF's reputation and protection of UNICEF's supporter (donor or celebrity) personal information.

UNICEF Standard on Exception to Website Information Security Policy Minimum Control (CF/ITSS/STANDARD/2015/002)

The purpose of this standard is to decrease organizational risks to UNICEF, in cases where compliance with UNICEF Policy on Information Security and or Website Information Security cannot be met. This standard applies to all UNICEF Websites that are hosted and/or supported by third party service providers that cannot comply with UNICEF's ICT/Information Security requirements.

This standard discusses website information security's main objectives: protecting UNICEF's brand, information security, UNICEF's reputation and UNICEF supporters' personal information. It also discusses responsibilities, minimum control requirements and accountabilities for implementation.

8.4.2. BCP/DR, Emergency Preparedness & Support

UNICEF Guidance on ICT Disaster Recovery for Field Offices (CF/ITSS/GUIDANCE/2015/001 Rev 15 August 2017)

The purpose of this guidance is to provide the necessary guidance to field offices on ICT Disaster Recovery in the Field Offices.

This guidance discusses recommended tools and response mechanisms for restoring voice communications, email and VISION services when the local ICT infrastructure and functions are no longer available due to a disaster/emergency. It focuses on the essential procedures that should be followed for efficient ICT disaster recovery planning in the field during an emergency. ICT is a vital component of the overall disaster recovery plan (DRP) and the larger office business continuity plan. This guidance does not provide instructions for developing a business continuity plan. Through the UNICEF Business Continuity Unit in OED, regional and country offices focal points will be trained and provided with tools for risk assessment and mitigation and business impact analysis, to assess the local situation and devise a business continuity plan.

Emergency Telecommunications Handbook

The purpose of this handbook is to ensure proper emergency preparedness, response planning and leadership in ICTs at the global, regional and local level. Ensuring this allows the realization of UNICEF's ICT mission to "transform and build partnerships with our stakeholders to successfully implement UNICEF programmers globally using innovative, technology-enabled solutions for better outcomes for children.

This extensive training manual was developed with the technical expertise of the ICT division, along with our partners and emergency responders.

This handbook discusses guidelines and detailed instructions to support teams in facilitating the delivery of effective emergency telecommunications at the field level. The document covers ICT emergency preparedness & response guidelines, high frequencies (HF) radios, very/ultra-high frequencies (VHF/UHF) radios, mobile satellite services (MSS), very small aperture terminals (VSAT) and IP technologies (LAN/WAN/VOIP and WiFi).

8.4.3. ICT Regulatory Management and Audit

UNICEF PROCEDURE ON THE REGULATORY FRAMEWORK (DFAM Policy 1, Supplement 4)

The purpose of this procedure is to set out the instruments governing the operations of UNICEF and accountabilities for developing and maintaining the regulatory instruments governing the operations of UNICEF. The Procedure applies to all programmatic, and administrative and operational aspects of the Organization’s work. This document should be referred to as the UNICEF Regulatory Framework.

8.5. Information Management Governance

8.5.1. Content Management

UNICEF Standard on Public Facing Website Hosting (ICTD/Standard/2019/001)

This Standard covers the standards on public facing website hosting for all UNICEF web properties required across UNICEF offices.

These Standards apply to all public-facing websites (sites which hold information for public consumption without authentication):

1. that are managed by, or on behalf of, UNICEF;
2. whether or not they are UNICEF-branded;
3. that are managed by, or on behalf of, UNICEF for multi-stakeholder partnerships (even if there is no UNICEF branding).
4. That are created/managed by/for all UNICEF offices – including Country Offices, Regional Offices and Headquarters Offices.
5. Offices, which have existing websites and their web hosting does not match with this new standard, may use a 2-year transition period after the effective date of this standard.

UNICEF Guidance on How to Produce Accessible Content

The purpose of the UNICEF ICTD User Guide on Producing Accessible Web and Multi-Media Content is to ensure widespread awareness of the requirements set out herein. This UNICEF ICTD User Guide focusses on creating accessible web content and developing accessible multi-media content. UNICEF ICTD believes that accessibility must be considered at every stage of the content development.

This guide discusses how to create accessible flash content, captions, transcripts and audio descriptions, future web accessibility (HTML5 <VIDEO>), web content accessibility and mobile web – making a website accessible both for people with disabilities and for mobile devices. The user guide also provides techniques and general approaches to rich internet application accessibility.

8.5.2. Information Access Management

See: UNICEF Standard on Information Security: Access Control (ICTD/STANDARD/2018/002)

8.5.3. IM Governance

UNICEF Standard on Conversion of Images into Text-Searchable Documents (ICTD/STANDARD/2018/012)

The purpose of this standard is to provide direction for digitization tools and instructions on conversion of images into text-searchable documents. This standard will help users convert electronic versions of text documents that lack the biggest advantage they can provide to the user – the ability to search within the contents of the document - into a format that supports this ability. This standard applies to all UNICEF offices and staff globally.

This standard discusses the electronic files that do not possess recognised text - that is, do not allow searching within the text of the document. Such files include images (.JPG, .GIF, .TIF, and .PNG) and PDF files, taken as photos (with a cell phone or camera), or created with the software that does not provide text recognition as a standard feature ("PDF as an image").

UNICEF Guidance on Digitization of Archival Material (ICTD/GUIDANCE/2018/001)

The purpose of this guidance is to provide assistance for digitization of archival material and other irregular objects (books, maps, etc.) held by UNICEF offices worldwide. Archival objects deteriorate with time. One approach to preserving them, in order to protect historical evidence of the work done by UNICEF over the years, and to provide continued long-term access to these objects, is to digitize them. Digitization (creation of a digital copy of an analog object) is a preservation technique that does not require specialized qualifications in archives. This guidance suggests best practices for digitization of archival materials to ensure the trustworthiness and reliability of the resulting digital copies.

This guidance discusses the types of archival material that can be destroyed, compares in-house versus outsourcing approaches to digitization, provides technical specification such as image resolution, colour, format standards and provides quality controls and storage information for the new digitized materials.

UNICEF Guidance on Scanning of Business Documents (ICTD/GUIDANCE/2018/002)

The purpose of this guidance is to provide assistance in creating digital copies of business documents by converting them from the original paper form (scanning) and summarizes relevant best practices and industry-accepted standards. These guidelines establish standards for digitization to ensure the trustworthiness and reliability of created digital copies and specify methods to assist in creating digitized records fit for long-term retention. They also suggest best practices for maintaining digitized copies after their creation and draw attention to disposal of the non-digital source records.

This guidance discusses planning and digitization, issues to consider when assessing the viability of digitization, indexing, scanning procedure, quality control and the disposition of original paper documents.

UNICEF Procedure on Information Management (ICTD/PROCEDURE/2019/001)

This Procedure outlines the principles of information management to which UNICEF is committed, and sets out general principles, expected practices and responsibilities. Together with other relevant regulatory instruments, this Procedure establishes the framework for information management in UNICEF. This Procedure supports efficient and effective management of UNICEF information assets for better decision-making, risk management, and the fulfilment of stakeholder commitments by ensuring that our information is: (a) Complete, authentic, accurate, and well organized; (b) Accessible to those who need it; (c) Captured, stored, retrieved, and destroyed or preserved according to need.

This Procedure applies to all UNICEF staff and authorized contractors; any recorded information created by UNICEF to support its work, or co-authored by UNICEF through partnerships, regardless of media and format (electronic or physical) and in any location globally, on or off premises or online; any recorded information received by or shared with UNICEF officially, and used by the organization to support its work; all UNICEF applications and systems, and systems supported by partners on behalf of UNICEF, holding UNICEF recorded information.

UNICEF Procedure on Destruction of Electronic Records (ICTD/PROCEDURE/2019/002)

Destruction is an important component of records management. It ensures that UNICEF retains records for as long as they are needed. When they are no longer needed, they are destroyed in an appropriate manner or transferred to the appropriate electronic repository for permanent retention. The destruction of electronic records that have passed their retention period is an essential step in maintaining a credible, reliable, and effective records system.

This procedure outlines the principles of electronic records destruction, identification of records that have passed their retention period, identification of the Office of the Primary Responsibility (OPR) and Approver, request for authorization of records destruction, authorization, destruction and logging destruction information.

This procedure applies to all UNICEF staff and offices globally; to all UNICEF electronic records and their metadata, regardless of file format. This Procedure does not apply to physical records.

UNICEF Procedure on Destruction of Physical Records (DFAM/PROCEDURE/2019/002)

Destruction is an important component of records management. It ensures that UNICEF retains records for as long as they are needed. When they are no longer needed, they are destroyed in an appropriate manner or transferred to the UNICEF Archives for permanent retention. The destruction of physical records that have passed their retention period, is an essential step in maintaining a credible, reliable, and effective records system.

This procedure outlines the principles of electronic records destruction; identification of records that have passed their retention period, identification of the Office of the Primary Responsibility (OPR) and Approver; compilation of the Records Destruction Form; request for authorization of records destruction, authorization, destruction activities and logging destruction information.

This procedure applies to all UNICEF staff and offices globally; to all UNICEF physical records, regardless of format (media type).

UNICEF Procedure on Sending Documents to Offsite Storage (DFAM/PROCEDURE/2019/005)

Offsite storage is generally an efficient and economical way to manage inactive records of different physical media. UNICEF offices that lack sufficient storage space for inactive records may consider storage of such documents in an offsite facility. This Procedure outlines actions and considerations to be taken by UNICEF staff when sending documents for storage outside of office premises. This Procedure does not cover management of an offsite storage facility, or administration of a contract with an offsite storage vendor.

This procedure applies to all UNICEF staff and offices globally; to all physical records, regardless of medium type, in custody of UNICEF offices.

UNICEF Procedure on Retention of Recorded Information (DFAM/PROCEDURE/2019/003)

This procedure describes how to ensure that UNICEF recorded information is retained by the organization for as long as it has business or organizational value. It outlines the principal retention periods, archival retention, limited retentions, special document types. This procedure forms part of the UNICEF Internal Controls Framework. It replaces any retention schedules and other policies, procedures, guidance or other regulations that deal with retention of any type of recorded information within UNICEF, other than the exceptions noted within this document.

This procedure applies to all UNICEF staff and authorized contractors; any recorded information created by UNICEF to support its work, or co-authored by UNICEF through partnerships, regardless of media and format (electronic or physical) and in any location globally, on or off premises or online; all types of documents and records, emails, audio-visual/multimedia content, etc.; any recorded information received by or shared with UNICEF officially, and used by the organization to support its work; all UNICEF applications and systems, and systems supported by partners on behalf of UNICEF, holding UNICEF recorded information.

UNICEF Procedure on User Access to the UNICEF Archives (DFAM/PROCEDURE/2019/007)

This document describes the procedures for accessing the UNICEF Archival holdings. The UNICEF Archives, as part of its mandate, has the duty of preserving and providing access to archival materials related to UNICEF's work for children and families worldwide. It outlines the how various user groups can access the UNICEF Archives.

This Procedure applies to all users of the UNICEF Archives. This Procedure can be used as guidance for managing access to archival holdings at any other UNICEF office globally.

UNICEF Procedure on Archival Material with Restricted Access (DFAM/PROCEDURE/2019/004)

This document describes the procedure to UNICEF staff managing archival holdings, on handling of materials containing sensitive information. UNICEF staff have a duty to ensure that sensitive (internal and/or confidential) information is not disclosed to unauthorized persons, as per UNICEF's Information Disclosure Policy and the UNICEF Standard on Information Security: Asset Management.

This Procedure applies to archival materials that contain internal and/or confidential information, as defined by UNICEF's Information Disclosure Policy and UNICEF Standard on Information Security: Asset Management; archival materials in custody of UNICEF Archives at NYHQ or archival facilities at all UNICEF offices globally; archival materials on any media, in any format, physical or electronic, and their archival description.

UNICEF Standard on Archival Description (DFAM/PROCEDURE/2019/006)

This standard establishes rules for consistent, appropriate, and self-explanatory description of archival materials across UNICEF. Archival description is essential for assisting users in finding desired information within archival holdings. The diverse nature of UNICEF archival materials, and their distribution across offices and archival facilities necessitate the existence of uniform descriptive rules, which will eliminate inconsistencies and confusion when searching for information.

This standard applies to archival materials in custody of UNICEF Archives at NYHQ or archival facilities at UNICEF offices globally. It also applies to UNICEF archival materials on any media, physical or electronic, and in any format.

UNICEF Procedure on Transferring Materials to UNICEF Archives (DFAM/PROCEDURE/2019/010)

This document describes the procedure that outlines the necessary steps UNICEF offices must take in order to identify materials with historical value for UNICEF in their custody and transfer them to the UNICEF Archives.

This procedure applies to materials being transferred to the UNICEF Archives by UNICEF offices, in any form, physical or electronic, and on any media. Where electronic content is concerned, this procedure only applies to materials stored and managed on shared and network drives, computer hard drives, etc., that is - outside of the designated UNICEF records repositories, e.g., Document Management System. Records in these repositories that merit permanent preservation are transferred to the archival electronic repository (i.e., Trusted Digital Repository) through automated workflows.

UNICEF Guidance on Handling of Physical Archival Materials (DFAM/GUIDANCE/2019/001)

The purpose of this Guidance is to enable UNICEF staff to appropriately handle archival materials in possession of any UNICEF office globally, in order to allow access to them while ensuring their preservation.

This Guidance applies to physical archival materials in possession of any UNICEF offices globally, it also applies to physical archival materials of any format, including, but not limited to, paper documents, audio-video materials, and/or special objects (artefacts). This Guidance, however, does NOT apply to electronic archival materials.

UNICEF Procedure on Archival Acquisition and Accessioning (DFAM/PROCEDURE/2019/011)

The purpose of this procedure is to establish the formal procedure of acquiring new materials into UNICEF Archives in New York HQ.

This procedure applies to UNICEF Archives in New York HQ, it can be used as guidance for acquiring new materials into any other UNICEF archival collection globally. This procedure also applies to all archival materials being acquired into the UNICEF Archives, in any format or media, including, but not limited to, paper, audio-visual, photographic, and electronic materials.

UNICEF Guidance on Management of Archival Collections (DFAM/GUIDANCE/2019/002)

The purpose of this Guidance is to enable UNICEF offices to correctly manage their archival collections, where a specialized archival facility and/or professional archival expertise are not available.

This Guidance applies to collections of archival materials in the possession of any UNICEF office globally as well as to physical archival materials of any format, including, but not limited to, paper documents, audio-video materials, and special objects (artefacts). This Guidance also applies to electronic archival materials stored on physical media (hard drives, CDs, flash drives, etc.). However, this Guidance DOES NOT apply to electronic archival materials stored in the designated UNICEF records repositories, e.g., the Document Management System. Records in these repositories that merit permanent preservation are transferred to the archival electronic repository (i.e., Trusted Digital Repository) through automated workflows.

9. REQUESTING AN EXCEPTION/WAIVER

Under extraordinary circumstances, offices may request an exception or waiver to the ICT Regulatory Documents that make up the ICT Baseline. Such requests shall include:

- The UNICEF IT policy, procedure, standard, and/or requirement to be waived or excepted.
- The reason and justification for the request must include elements such as: Risk Assessment; Cost-Benefit Analysis; Business Impact Assessment; Identification of compensating controls/actions; Proposed period of time for the exception; Proposed date by which the Office will be compliant with the regulatory document, security control, and/or requirement.

Offices may request an exception to a new or revised policy or other prescriptive document via email to pmo@unicef.org in line with the requirements cited above.

- The CIO shall evaluate the waiver request and the concurrence and either approve or disapprove the request accordingly.
- This waiver process applies only to those regulatory documents for which the Office of the UNICEF CIO is responsible. For exceptions to requirements in UNICEF regulatory documents for which the UNICEF CIO is not responsible, the requester shall follow the process outlined in the related UNICEF regulatory document.
- Requesters in the field may appeal first to the Regional Chief of ICT and then to the CIO for a review of regional decisions.
- All approved exceptions to an established IT policy, procedure, and standard will be noted in the ICT Baseline facility.
- The non-approval of requests for exceptions and waivers shall be communicated to the requester.

ANNEX I: ICTD Regulatory Document Development/Update Workflow

Step 1: Create New or Update existing document

New document creation: Responsible Manager drafts the regulatory document.
Update existing document**:** Policy Management Reviews and change policy status to "Draft".

In either case, use the appropriate template to create/update a regulatory document.

- **Step 1.1:** *Stakeholders' contribution:* The Responsible Manager identifies key stakeholders and co-author the document in the system. Add the key stakeholders' names and stakeholders review date in ICT Policy Management tool and select "Stakeholders Review".
- **Step 1.2:** *Submit for Endorsement:* After the document is consulted with the key stakeholders and finalized, submit to the Document/Business Owner for Endorsement.

Step 2: Endorsement Stage

- When endorsed, the policy quality review process will be carried out and the document work-flowed for Management Review.
- If change is requested by the Endorser, the document goes back to the Responsible Manager.

Step 3: Management Review Stage

All members of Management Review group will be notified to provide comments/feedback.

- After the Management Review date, the policy quality management will coordinate with the Responsible Manager to take action on the feedback/comments received from Management Reviewers.
- Policy Management will submit the document to the CIO for Approval.

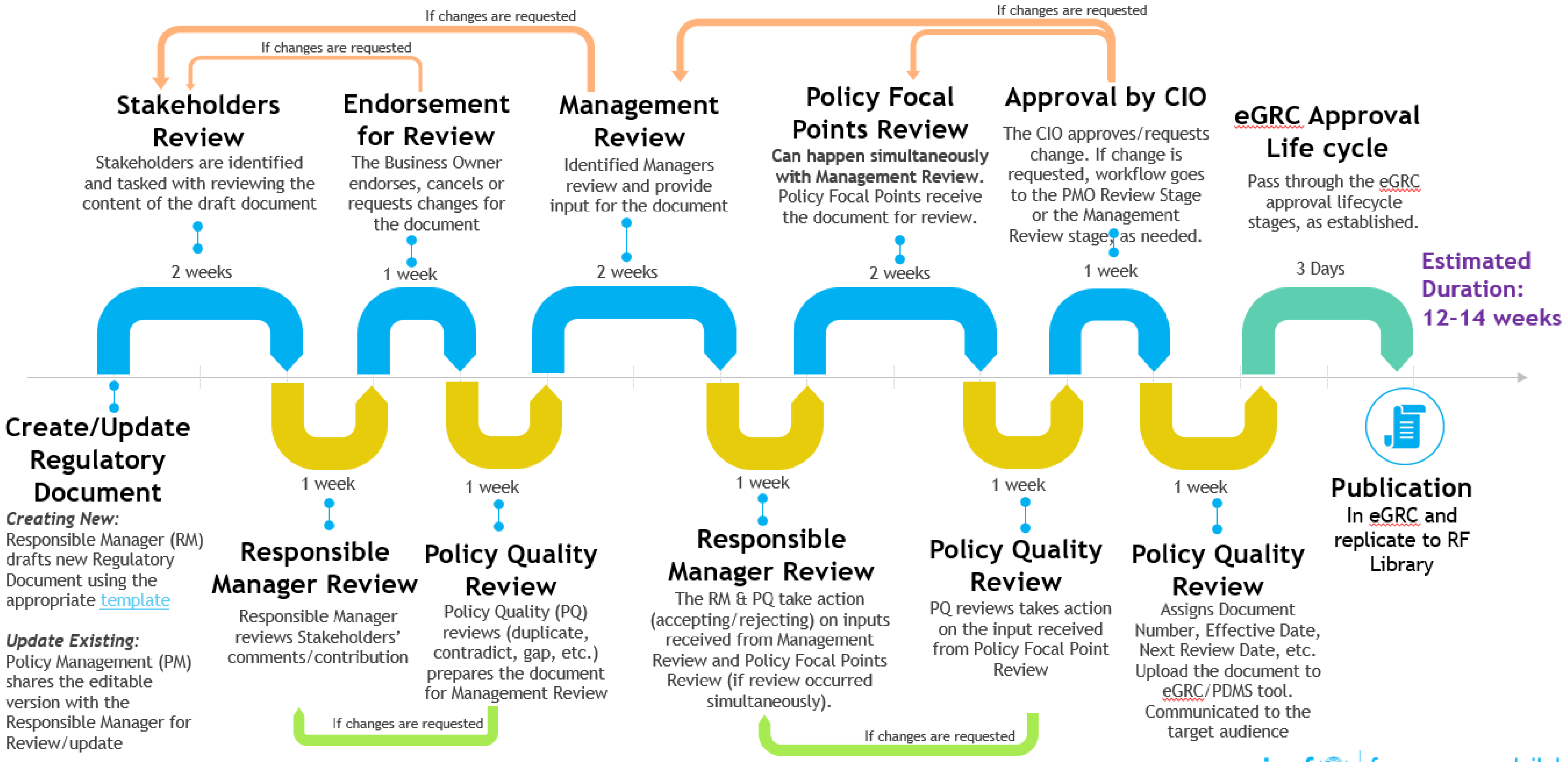
Step 4: Business Owner - CIO Approval

- When approved, Policy Management will prepare the document for publication by assigning a document number, effective date, mandatory review date, etc.
- If change is requested, Policy Management will take necessary action, and workflow to the appropriate stage.

Step 5: Regulatory document is Published

- Policy Management will edit the document properties: set effective and next mandatory review dates and assign a document number.
- Policy Management will upload the approved document to the eGRC PDMS tool for further processing. Once the document passes through the eGRC approval lifecycle and published in eGRC, the approved document will be replicated to the RF Library.
- Policy Management team in consultation with the Document Owner can send out communication to the target audiences.
- If the document warrants translation to other UN languages (French and Spanish) Policy Management secures funding and arrange translation of the document, usually through the DOC Editors.

ICT Regulatory Documents Creation and Update Process



Create/Update Regulatory Document

Creating New: Responsible Manager (RM) drafts new Regulatory Document using the appropriate template

Update Existing: Policy Management (PM) shares the editable version with the Responsible Manager for Review/update

Stakeholders Review — 2 weeks

Stakeholders are identified and tasked with reviewing the content of the draft document

Responsible Manager Review — 1 week

Responsible Manager reviews Stakeholders' comments/contribution

Endorsement for Review — 1 week

The Business Owner endorses, cancels or requests changes for the document

Policy Quality Review — 1 week

Policy Quality (PQ) reviews (duplicate, contradict, gap, etc.) prepares the document for Management Review

Management Review — 2 weeks

Identified Managers review and provide input for the document

Responsible Manager Review — 1 week

The RM & PQ take action (accepting/rejecting) on inputs received from Management Review and Policy Focal Points Review (if review occurred simultaneously).

Policy Focal Points Review — 2 weeks

Can happen simultaneously with Management Review. Policy Focal Points receive the document for review.

Policy Quality Review — 1 week

PQ reviews takes action on the input received from Policy Focal Point Review

Approval by CIO — 1 week

The CIO approves/requests change. If change is requested, workflow goes to the PMO Review Stage or the Management Review stage, as needed.

Policy Quality Review — 1 week

Assigns Document Number, Effective Date, Next Review Date, etc. Upload the document to eGRC/PDMS tool. Communicated to the target audience

eGRC Approval Life cycle — 3 Days

Pass through the eGRC approval lifecycle stages, as established.

Publication

In eGRC and replicate to RF Library

Estimated Duration: 12-14 weeks

unicef for every child