UNICC Information Security Policy
POL-0013

Version 2.2

This document outlines the Information Security Policy for the UNICC

12th January 2023

Status: ***4 - Approved***

Contents

1 Overview

1.1 Copyright

1.2 Confidentiality

This document contains information regarding the United Nations International Computing Centre and its customers and is **Public unclassified**.

1.3 Approval History

20/07/2020 15:24 - SONI Tima - Approved.
This policy was approved by the SMG dated 12 June 2020.
21/07/2020 13:43 - MAGGIORE Fabio - Approved.
10/01/2022 15:51 - CPI Librarians - Reviewed.
10/01/2022 17:01 - MAGGIORE Fabio - Approved.
12/01/2023 08:50 - CPI Librarians - Reviewed.
12/01/2023 09:35 - SONI Tima - Approved.
12/01/2023 10:04 - MAGGIORE Fabio - Approved.

1.4 Contact

Please refer all inquiries regarding this document to UNICC Service Desk, servicedesk@unicc.org.

1.5 Related Documents and Tools

REF	Document/Record	Description	Location
1	ISO/IEC 27001:2013	ISO/IEC 27001 requirements	n/a
2	UNICC Enterprise Risk Management Policy	UNICC Enterprise Risk Management Policy	Staffnet – GRC Site

1.6 Document History

Version	Day	Person	Action
1.0	11/01/2016	Toby Felgenner	First version for distribution.
1.1	13/12/2016	Toby Felgenner	Review, minor corrections and minor update
1.2	27/06/2017	Toby Felgenner	Review, minor corrections and minor update
1.3	13/09/2017	Toby Felgenner	Review, minor corrections and minor update
1.4	17/09/2018	Toby Felgenner	Review and minor updates
1.5	23/09/2018	Toby Felgenner	Minor updates
2.0	03/07/2020	Fabio Maggiore	Document reviewed including updates and reviews by Tima Soni and Security Management Group (SMG)
2.1	10/01/2022	Carlos Aleixandre	Updated with new classification and label
2.2	22 December 2022	Carlos Aleixandre	Minor changes: update logo, unit names and document classification to public.

2 Introduction

2.1 Background

2.1.1. Pursuant to General Assembly Resolution 2741 (XXV) of 17 December 1970, the Untied Nations International Computing Center (UNICC) was created as an inter-organization facility to provide a common Electronic Data Processing Services. The UNICC delivers a broad range of IT services and a state of the art secure computing environment. As such, information security is important and is of significant value to the mission of UNICC.

2.1.2. This information security policy (referred to as "the policy" in this document) provides a mechanism to establish a framework to protect UNICC's information assets from security threats and minimize the impact of security incidents.

2.1.3. The policy is supported by specific policies and standards. Related information security documents, such as standards and procedures, govern in conjunction with this policy[1].

2.2 Purpose

2.2.1. This policy determines the information security risk posture of UNICC and provides the basis to establish the framework for the Information Security programme that is designed to protect UNICC's information assets from all threats, whether internal or external, deliberate or accidental.

2.2.2. This policy establishes UNICC's commitment to information security by preserving the confidentiality, integrity and availability of all physical and electronic information assets used throughout the business and especially information entrusted by customers.

- **Confidentiality** – making sure that the information is available only to those who have a genuine need to access it.
- **Integrity** – making sure that the information is protected from unauthorised and accidental modification and/or deletion.
- **Availability** – making sure that the information is available to the people who need it at the time they need it.

2.3 Objective

2.3.1. The objective of the Information Security Policy is to:

- Manage information security risks to an acceptable level.
- Support UNICC's mission by facilitating efficient use of information in a secure and responsible manner.
- Maintain competitive edge and reputation.
- Ensure compliance with internationally recognized standards (e.g. ISO 27001:2013)

2.4 Scope and applicability

2.4.1. This policy applies to all UNICC staff and non-staff that use and/or have access to UNICC information assets.

[1] Refer to Annex A for a list of related policies and standards.

2.4.2. This policy applies to all information assets owned by and/or managed by UNICC for its Partners.

2.4.3. This policy applies to all UNICC locations.

3 Policy

3.1 Statements

3.1.1. UNICC staff and non-staff users must respect the legitimate interests of the Organization. When accessing UNICC's information assets, they must:

- Take adequate precautionary measures to protect the confidentiality, integrity, and availability of information assets.
- Take adequate precautionary measures to protect the reputation of the Organization.
- Use the information assets only for their intended business purpose(s).
- Conduct themselves in accordance with this policy, the UNICC Acceptable Use Policy and the Standards of Conduct for The International Civil Service.
- Successfully complete mandatory Information Security Trainings.

3.1.2. Before procurement, development of any new capabilities, or making any significant change in the computing environment, the information or system owner must ensure that a risk assessment is conducted under the guidance of a Cybersecurity Division (CS) representative. The assessment must focus on identifying risks associated to the reputation of UNICC and to the confidentiality, integrity and availability of UNICC's information assets.

3.1.3. The UNICC Enterprise Risk Management Policy (and related procedures) must be followed for mitigating information security risks. The risks identified must be captured in a formal risk register.

3.1.4. Human Resources security practices must be followed all the time (prior to the staff or non-staff employment, during the service and upon contract termination). UNICC must ensure that confidentiality requirements and intellectual property rights survive after contract termination.

3.1.5. All UNICC information assets must be classified according to their sensitivity level ensuring that they receive an appropriate level of protection. Distinct handling, distribution, labeling, and review procedures must be established for each classification.

3.1.6. Cryptographic keys used to encrypt and decrypt sensitive information must be carefully managed and controlled with processes for generating, distributing, storing, losing, compromising or damaging keys.

3.1.7. All access to UNICC information assets must be based on the principles of "least privilege", "need to know" and in accordance with distinct procedures established to grant such access.

3.1.8. Information about user activity must be monitored and logged anonymously, wherever possible, to protect the privacy of users unless such information is being logged or monitored for investigative purposes with authorization from UNICC Director's. System logs or application audit trails must not be disclosed to any person outside the team of

individuals who ordinarily view such information in order to perform their jobs or investigate information.

3.1.9. Relevant logging and monitoring for the purposes of detecting security threats must be enabled.

3.1.10. Security incident response procedures must be developed and maintained to accurately identify, contain and remediate information security incidents.

3.1.11. Controls to limit the likelihood of cyber-attacks and security incidents to occur must be implemented. These controls must be regularly reviewed and updated to address cyber threats relevant at any given point.

3.1.12. All UNICC systems must have an adequately-staffed process for expediently and regularly identifying, reviewing and remediating security vulnerabilities.

3.1.13. Traditional software development and modern DevOps (CI/CD Pipelines) practices must ensure that security is an integral part of developing applications. These practices must continuously integrate security in development pipelines, regularly perform static and dynamic code assessments and continuous monitoring thereafter.

3.1.14. All UNICC information assets must be adequately protected against corruption or loss. Backup and recovery procedures must be configured according to their criticality.

3.1.15. Business continuity plans must be part of any IT-related solution to support the Organization during high-impact incidents. Business continuity plans are maintained and periodically tested.

3.2 Governance

3.2.1. The Cybersecurity Division (CS) is responsible for administering this policy. Requests for exceptions to this policy should be addressed to the Chief, Cyber Security Section via the Service Desk.

3.2.2. A security management group (SMG) is established to direct, monitor and communicate the information security strategy and to provide assurance that identified risks are being addressed. The SMG governance is defined in the SMG Terms of Reference.

3.3 Communication

3.3.1. Any updates and/or changes to this Policy or related standards must be communicated to staff on a timely basis. This policy will undergo review on an annual basis.

3.4 Exceptions

3.4.1. Exceptions to the requirements of this policy may exist:

- Any deviation from Information Security Policy and related standards must be documented and submitted for review to the Security Management Group (SMG).
- Exceptions will be undertaken by the Director's Office and documentation of approval will be retained.
- If the exception request involves a high or very high risk, as identified by the Chief, Cyber Security Section, clearance should be sought from the UNICC Director.
- Exceptions must be properly recorded and have fixed time and limited duration.

3.5 Compliance

3.5.1. A staff or non-staff member who breaches the UNICC Information Security Policy and related standards may be deemed to have failed to observe the standards of conduct for staff.

3.5.2. Where such misconduct results in loss or damage to the confidentiality, integrity or availability of UNICC information assets, the staff member may be subject to disciplinary measures under Article X of the Staff Regulations and Section 11 of the Staff Rules.

3.5.3. Non-staff members are subject to similar measures under the terms and conditions of their contract and and/or signed Non-Disclosure Agreement (NDA).

3.5.4. Any matter of concern relating to this policy should be reported to the Service Desk or to the UNICC Director who will investigate the allegations and refer them to the Human Resources and the WHO Office of Internal Oversight Service.

3.5.5. UNICC must verify compliance to this policy through various methods, including but not limited to, reporting tools, internal and external audits.

4 Document Owner and Approval

4.1 Document Owner and Approval

The Cybersecurity Governance Unit (CSG) is the owner of this document.

The Cybersecurity Governance Unit (CSG) is responsible for ensuring that this document is reviewed in line with the requirements of the Information Security Management System (ISMS).

A current version of this document is available to UNICC users on the StaffNet website in the relevant folder on the UNICC Integrated Management System site.

5 Annex A – Related Standards

In line with the third statement of section 2.1 above, this policy is supported by the following standards:

- STD-1200 - UNICC Acceptable Use Standard
- STD-1201 - UNICC Information Classification, Labeling and Handling Standard
- STD-1202 - UNICC Information Security Risk Management Standard
- STD-1203 - UNICC Identity and Access Management Standard
- STD-1204 - UNICC Information Security Awareness, Training, and Education Standard
- STD-1990 - UNICC Vulnerability Management Standard
- STD-1205 - UNICC Information Security Incident Management Standard
- STD-1206 - UNICC Asset Management Standard
- STD-1207 - UNICC Encryption Standard
- STD-1208 - UNICC Network Security Standard
- STD-1209 - UNICC Secure Coding and Application Security Standard
- STD-1210 - UNICC Security Log Collection, Analysis, and Retention Standard
- STD-1211 - UNICC Secure Configuration Standard
- STD-1213 - UNICC Third Party Security Standard
- STD-1214 - UNICC Cloud Security Standard
- STD-1215 - UNICC Physical Security Standard
- STD-1216 - UNICC End User and BYOD Standard
- STD-1217 - UNICC Password Management Standard

6 Annex B – Roles and Responsibilities

Role	Responsibilities
Users	• Use Information assets in accordance with this policy, the Acceptable Use Policy, the Standards of Conduct for The International Civil Service; • Protect their access credentials for IT systems and not disclose them; • Report any security incidents to the Service Desk or to the Cybersecurity Division (CS); • Store confidential information only on UNICC authorized equipment, environments and/or services; • Do not disclose UNICC internal information including configurations, report or any other UNICC produced information to external parties without prior authorization of the data owner; • Do not disclose Security Incident information or Security configuration to external parties without prior authorization from Cybersecurity;
Unit Heads and Team Leaders	• Oversee the acceptable use of information assets; • Ensure that all employees within their supervision complete the Information Security Awareness training; • Ensure staff are aware of their responsibilities under this policy and the consequences of inappropriate behaviour; • Escalate any policy breach confidentially to Cybersecurity; • Inform the Service Desk when employees leave their supervision, whether they are transferred, change their roles or leave the Organization;
HR	• Provide in timely matter information to UNICC Service Desk regarding staff and consultants appointment, transfer, termination so that appropriate steps can be taken to create, change or revoke access rights on the ICT systems; • Ensure that Information Security Awareness training is made compulsory for staff members and consultants and its attendance recorded in the staff folders;
Chief, Cybersecurity Division (CS)	• Define and manage the strategic direction of Cybersecurity and the implementation and operation of security measures; • Evaluate and provide reasonable assurance that risk management, control, and governance systems are functioning as intended and will enable UNICC's objectives and goals to be met; • Report risk management issues and identified internal controls deficiencies to the Security Management Group (SMG); • Maintain and update the Information Security Roadmap and perform the yearly Risk Assessment; • Develop/maintain a security and control framework that consists of standards, measures, practices and procedures; • Work closely with senior management as their security and compliance focal point; • Oversee the implementation of and compliance with this policy, including systems to assist in the monitoring and management of compliance; • Provide appropriate support and guidance to assist employees and supervisors fulfil their responsibilities under the Information Security Policy; • Develop and update the Information Security Awareness Programme, including training and control that staff has actually attended;

	• Monitor general business trends and technology developments, new threats and vulnerabilities and takes the necessary remediation/preventive actions; • Facilitate independent reviews and assessments to ensure the continuing suitability, adequacy, and effectiveness of an UNICC's approach to managing information security; • Provide recommendations for improving UNICC's operations, in terms of both efficient and effective performance; • Provide technical assistance in the resolution of security incidents and reduction of risks; • Ensure implementation of and subsequent compliance with UNICC's Information Security requirements from all 3rd party ICT service providers to the UNICC;
UNICC Director	• Responsible for the overall implementation of the policy; • Monitor the execution and impact of the policy on the Organization; • Compliance with relevant internal rules and legislation on data.