الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

National Information Security Compliance Framework (NISCF) – General Policy for National Certification

[NCSA-NISCF-CERT-GPNC]

Policy

National Cyber Security Agency (NCSA)

December 2023

V 1.0

C0 – Public / PS1 – Non-Personal Data (Non-PD)

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Document Control

Document Details	
Document ID	NCSA-NISCF-CERT-GPNC
Version	V 1.0
Confidentiality labelling	C0 – Public / PS1 – Non-Personal Data (Non-PD)
Abstract	This document is the General Policy for National Certification developed by the National Cyber Security Agency (NCSA) with the intended usage in the operation of National Information Security Compliance Framework (NISCF) Certification Services. This document provides high-level direction for requirements definition for NISCF Certification Services.

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

DISCLAIMER / LEGAL RIGHTS

National Cyber Security Agency (NCSA) has designed and created this publication, titled "National Information Security Compliance Framework (NISCF) – General Policy for National Certification" - V 1.0 - C0 – Public / PS1 – Non-Personal Data (Non-PD), in order to provide high-level direction for requirements definition for NISCF Certification Services.

NCSA is responsible for the review and maintenance of this document.

Any reproduction of the present document either in part or full and irrespective of the means of reproduction; shall acknowledge NCSA as the source and owner of the "National Information Security Compliance Framework (NISCF) – General Policy for National Certification".

Any reproduction concerning this document with intent of commercialization shall seek a written authorization from the NCSA. NCSA shall reserve the right to assess the functionality and applicability of all such reproductions developed for commercial intent.

The authorization from NCSA shall not be construed as an endorsement of the developed reproduction and the developer shall in no way publicize or misinterpret this in any form of media or personal / social discussions.

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

LEGAL MANDATE(S)

Based on Emiri Decree No 1 of year 2021, National Cyber Security Agency (NCSA) – National Cyber Governance and Cyber Assurance Affairs (NCGAA) is the entity responsible for issuing certificates for Technology and Information Security service providers and Certificates of Compliance with National Information Security standards and policies.

This Policy has been prepared to take into consideration the current applicable laws of the State of Qatar. If a conflict arises between this document and the laws of Qatar, the latter shall take precedence. Any such term shall, to that extent be omitted from this Document, and the rest of the document shall stand without affecting the remaining provisions. Amendments, in that case, shall then be required to ensure conformance with the relevant applicable laws of the State of Qatar.

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Table of Contents

1. Introduction 6

2. Purpose and Scope 7

2.1. Purpose 7

2.2. Scope 7

3. Key Definitions 8

4. Policy Statements 9

4.1. General 9

4.2. Information 10

4.3. Certification Operation 12

4.4. Complaint and Appeal 18

5. Compliance and Enforcement 19

5.1. Compliance Process 19

5.2. Roles and Responsibilities 19

5.3. Transitioning and effective date 19

5.4. Exceptions and deviations 19

6. Annexes 21

6.1. Acronyms 21

6.2. Reference 21

1. Introduction

National Cyber Security Agency (NCSA) created its Certification Services to provide assurance that organizations comply and conform with specific Cyber Security requirements defined in National and International Standards that are adopted by NCSA.

In effort to improve the Certification Services, NCSA developed this document, titled "National Information Security Compliance Framework (NISCF) – General Policy for National Certification" - V 1.0 - C0 – Public / PS1 – Non-Personal Data (Non-PD), to provide the cyber space with clearer overall principles and objectives on the Certification Services.

2. Purpose and Scope

2.1. Purpose

The purpose of this document is to provide high-level direction for requirements definition for NISCF Certification Services.

2.2. Scope

The General Policy for National Certification applies to all Certification Services that are offered by NCSA under the NISCF.

3. Key Definitions

The terminologies used in this policy are consistent with the definitions provided in the NCSA-NISCF-CERT-GTXD (General Taxonomy Document for National Certification - Public).

4. Policy Statements

4.1. General

4.1.1. Certification Services Authority (Certification Body)

4.1.1.1. Certification Services Accountability

4.1.1.1.1. As per the Emiri Decision No.1 of the Year 2021, National Cyber Security Agency (NCSA) is the Certification Body for NISCF's Certification Services and therefore, is solely responsible for, and remain fully accountable on related Certification decisions.

4.1.1.1.2. NCSA can authorize one or more defined part(s) of its structure to act as the Certification Body for NISCF Certification Services.

4.1.1.1.3. The Certification Body is responsible and accountable for retaining and maintaining evidences to demonstrate conformance to the NISCF Certification Services requirements.

4.1.1.2. Certification Services Fairness

4.1.1.2.1. The Certification Body commits to impartiality and objectivity of the NISCF Certification Services, through:

- Establishing a risk management system to identify, evaluate, mitigate and monitor potentially arising conflict of interests impacting the Certification Body itself, persons in charge with its governance and / or management, employees, sub-contractors and partners; and
- Implementing administrative, technical and financial safeguards.

4.1.1.3. Certification Services Continuity

4.1.1.3.1. NISCF's Certification Services finances and resources are defined and managed by the Certification Body in order to guarantee their continuity in the light of its strategy and objectives.

4.1.2. Certification Services requirements

4.1.2.1.1. The Certification Body defines and maintains the NISCF's Certification Services requirements.

4.1.2.1.2. The Certification Body determines, solely or in collaboration with other entities, the means to document and communicate the NISCF's Certification Services requirements for the different stakeholders.

4.1.2.1.3. The Certification Body determines the period of validity of a Certificate of Compliance granted under the NISCF's Certification Services.

4.1.2.1.4. The Certification Body determines the fees associated with NISCF's Accreditation Services, their applicability, payments methods and period.

4.1.3. Certification Services Agreements

4.1.3.1.1. Relationships between stakeholders in NISCF's Certification Services are governed by legally enforceable agreements established between the different stakeholders, individually or collectively.

4.2. Information

4.2.1. Public Information

4.2.1.1.1. NISCF's Certification Services information are publicly made available by the Certification Body.

4.2.1.1.2. The Certification Body can decide to provide certain NISCF's Certification Services information only upon request at the condition that the non-publicly available information does not significantly impact the NISCF's Certification Services understanding by the cyber space.

4.2.2. Certifications records

4.2.2.1.1. The Certification Body defines the content and format of NISCF's Certification records.

4.2.3. Certification reference and usage

4.2.3.1.1. The Certification Body defines the terms and conditions for the usage of NISCF's Certification symbols, title, credentials or any other demarcation.

4.2.3.1.2. The Certification Body owns the NISCF's Certification symbols, marks and logos.

4.2.3.1.3. The Certification Body can license the use of the NISCF's Certification symbols, marks and logos to a third-party.

4.2.4. Confidentiality

4.2.4.1.1. The Certification Body is solely accountable and responsible for the confidentiality of all information obtained directly from the data owner or created by the Certification Body during the operation of NISCF Certification Services, at all organization's levels and individuals acting on its behalf.

4.2.4.1.2. For information obtained during the operation of NISCF Certification and shared with a third-party for the purpose of NISCF Certification operation, the Certification Body is jointly responsible, along with the third-party, of the confidentiality of such information.

4.2.5. Communication with stakeholders

4.2.5.1.1. The Certification Body defines and provides the information that is deemed required to the NISCF's Certification stakeholders.

4.2.5.1.2. The Certification Body determines communication methods and means, that are deemed adequate to communicate any change of the NISCF's Certification Services information to the stakeholders.

4.2.5.1.3. The Certification Body defines the terms and conditions for NISCF Certification stakeholders to communicate changes to the Certification Body and / or other stakeholders.

4.2.6. Security

4.2.6.1.1. The Certification Body defines and enforces information security requirements related to NISCF Certification Services for all stakeholders.

4.3. Certification Operation

4.3.1. Application

4.3.1.1. Request for Certification

4.3.1.1.1. NISCF's Certification Services can only be provided after a formal request for Certification to the Certification Body.

4.3.1.1.2. The Certification Body defines the requirements and information needed for requesting NISCF's Certification Services.

4.3.1.1.3. NISCF's Certification Services application requirements have for main purpose to clearly identify and delimit the scope for the NISCF's Certification Services request.

4.3.1.2. Request review

4.3.1.2.1. The Certification Body reviews the request for NISCF's Certification Services to confirm the scope conformance to NISCF's Certification Services request requirements and with laws, policies and standards requirements related to the NISCF's Certification Services requested.

4.3.1.2.2. The Certification Body is to provide the applicant and / or other stakeholders related to a NISCF's Certification Services request with a formal acceptance or rejection and / or feedbacks on its NISCF's Certification Services request.

4.3.2. Audit, assessment, evaluation, and examination

4.3.2.1. Audit, Assessment, Evaluation and Examination Bodies (AAEEBs)

4.3.2.1.1. The Certification Body determines eligible Audit, Assessment, Evaluation and Examination Bodies (AAEEBs) that can be engaged in the NISCF's Certification Services.

4.3.2.1.2. The Certification Body can perform audits, assessments, evaluations, and examinations for part(s) or the complete scope, with its own resources, if it has the necessary capability and capacity required to undertake.

4.3.2.1.3. The assigned AAEEB is responsible to identify, assess, mitigate, and monitor potentially arising conflict of interests that could impact impartiality and objectivity of the NISCF's Certification Services.

4.3.2.2. Planning

4.3.2.2.1. The Certification Body is responsible for planning the audits, assessments and evaluations.

4.3.2.2.2. The Certification Body can delegate the planning activities to the engaged AAEEBs, to accommodate specific requirements of a NISCF's Certification Service.

4.3.2.3. Execution

4.3.2.3.1. The engaged AAEEBs are responsible for executing the audits, assessments, evaluations, and examinations as per the defined plans.

4.3.2.3.2. The engaged AAEEBs are responsible for gathering sufficient and appropriate evidence to reach the level of assurance required to formulate conclusions regarding the scope for a NISCF's Certification Services request.

4.3.2.4. Reporting

4.3.2.4.1. The engaged AAEEBs are responsible to report to the Certification Body and / or other stakeholders related to a NISCF's Certification Services request, the results of the audits, assessments, evaluations, and examination.

4.3.2.5. Independent review

4.3.2.5.1. The Certification Body is responsible for the independent review of AAEEBs' audits, assessments, evaluations, and examination results related to a NISCF's Certification Services request.

4.3.3. Certification Decision

4.3.3.1. Types of Certification Decision

4.3.3.1.1. The Certification Body determines the types of Certification Decisions available to be taken at different stage of the NISCF's Certification lifecycle, considering the NISCF's Certification Services applied for.

4.3.3.2. Responsibility of Certification Decision

4.3.3.2.1. The Certification Body is responsible for the Certification Decisions related to the NISCF's Certification Services.

4.3.3.2.2. The Certification Body cannot delegate Certification Decisions related to the NISCF's Certification Services.

4.3.3.2.3. Certification Decisions related to the NISCF's Certification Services can be jointly made with other organizations if the NISCF Certification Services in question have been jointly developed with the above-mentioned organizations.

4.3.3.3. Initial Certification Decision

4.3.3.3.1. The Certification Body is responsible to provide the applicant for the NISCF's Certification Services, the Certified Organization and / or other stakeholders related to a NISCF's Certification Services request or Certificate of Compliance with a formal Certification decision.

4.3.4. Maintenance, Suspension, Reinstatement, Changes affecting the Scope, Scope reduction, Scope expansion, Termination, Withdrawal and Expiry

4.3.4.1. Maintenance

4.3.4.1.1. The Certification Body is responsible for determining the maintenance requirements for NISCF's Certification Services.

4.3.4.1.2. Certificate of Compliance granted under the NISCF's Certification Services are subject to maintenance, unless specified otherwise by specific NISCF's Certification Services requirements in order to align and / or conform with best practices and standards in the cyber security area of expertise of the above-specified NISCF's Certification Services.

4.3.4.2. Suspension

4.3.4.2.1. Certificate of Compliance granted under the NISCF's Certification Services can be subject to suspension by the Certification Body if certain conditions are met.

4.3.4.2.2. The Certification Body defines the conditions under which the Certificate of Compliance granted under the NISCF's Certification Services can be suspended.

4.3.4.3. Reinstatement

4.3.4.3.1. Reinstatement of suspended Certificate of Compliance under the NISCF's Certification Services can only be performed by the Certification Body if the conditions that led to the suspension has been resolved.

4.3.4.4. Changes affecting the Scope

4.3.4.4.1. The Certification Body can introduce changes (new or updated requirements) to existing NISCF's Certification Services that may affect active Certificates of Compliance.

4.3.4.4.2. The Certification Body will communicate, through appropriate means, the changes introduced and the associated requirements to conform with the changes.

4.3.4.4.3. The Certification Body is responsible for ensuring that active Certificates of Compliance conform with the changes.

4.3.4.4.4. The Certification Body is responsible for providing means for the NISCF's Certification Services stakeholders to report changes that may affect active Certificates of Compliance.

4.3.4.4.5. The Certification Body is responsible for assessing the changes and defining the necessary actions.

4.3.4.4.6. The Certification Body is responsible for ensuring that necessary actions are implemented.

4.3.4.5. Scope reduction

4.3.4.5.1. The Certification Body is responsible for determining conditions under which scope reduction is permissible for NISCF's Certification Services.

4.3.4.5.2. The Certification Body defines if a specific NISCF's Certification Services allows for scope reduction in order to align and / or conform with best practices and standards in the cyber security area of expertise of the above-specified NISCF's Certification Services.

4.3.4.6. Scope expansion

4.3.4.6.1. The Certification Body is responsible for determining conditions under which scope expansion is permissible for NISCF's Certification Services.

4.3.4.6.2. The Certification Body defines if a specific NISCF's Certification Services allows for scope expansion in order to align and / or conform with best practices and standards in the cyber security area of expertise of the above-specified NISCF's Certification Services.

4.3.4.7. Termination

4.3.4.7.1. The Certification Body is responsible for determining the means available for a Certified Organization to request termination of a NISCF's Certificate of Compliance.

4.3.4.7.2. The Certified Organization can request for a termination of NISCF's Certificate of Compliance, only before the expiry of the period of validity of the NISCF's Certificate of Compliance.

4.3.4.7.3. The Certification Body shall conform to the Certified Organization request and terminate the NISCF's Certificate of Compliance.

4.3.4.8. Withdrawal

4.3.4.8.1. Certificate of Compliance granted under the NISCF's Certification Services can be subject to withdrawal by the Certification Body if certain conditions are met.

4.3.4.8.2. The Certification Body defines the conditions under which the Certificate of Compliance granted under the NISCF's Certification Services can be withdrawn.

4.3.4.9. Expiry

4.3.4.9.1. Certificate of Compliance granted under the NISCF's Certification Services have a defined period of validity when issued by the Certification Body.

4.3.4.9.2. The Certification Body defines the period of validity for NISCF's Certification Services.

4.3.4.9.3. Certificate of Compliance granted under the NISCF's Certification Services that has not been subject to a request for Re-Certification, by the Certified Organization or did not conform with Re-Certification requirement, expires at the end of the period of validity.

4.3.5. Re-Certification

4.3.5.1.1. The Certification Body is responsible for determining the means available for a Certification Organization to request a NISCF's Certificate of Compliance extension of the period of validity through Re-Certification.

4.3.5.1.2. The Certification Body is responsible for determining the Re-Certification requirements for the NISCF's Certification Services.

4.4. Complaint and Appeal

4.4.1. Complaint

4.4.1.1.1. The Certification Body is responsible for determining the means available for the NISCF's Certification Services stakeholders to lodge a complaint about the NISCF's Certification Services and its operation.

4.4.1.1.2. The Certification Body determines the conditions of acceptance, review and communication of complaints related to the NISCF's Certification Services.

4.4.1.1.3. The Certification Body is solely responsible for complaints' related decisions for the NISCF's Certification Services.

4.4.1.1.4. The Certification Body ensures that complaints handling related to the NISCF's Certification Services conform to principles defined in section **4.1.1.2**.

4.4.2. Appeal

4.4.2.1.1. The Certification Body is responsible for determining the means available for the NISCF's Certification Services stakeholders to appeal the NISCF's Certification Services decisions.

4.4.2.1.2. The Certification Body determines the conditions of acceptance, review and communication of appeals related to the NISCF's Certification Services.

4.4.2.1.3. The Certification Body is solely responsible for appeals' related decisions for the NISCF's Certification Services.

4.4.2.1.4. The Certification Body ensures that appeals handling related to the NISCF's Certification Services conform to principles defined in section **4.1.1.2**.

5. Compliance and Enforcement

5.1. Compliance Process

All stakeholders to the NISCF's Certification Services shall conform with the statements defined in this policy.

5.2. Roles and Responsibilities

National Cyber Governance and Assurance Affairs (NCGAA) is responsible for enforcing and monitoring conformance to this policy.

5.3. Transitioning and effective date

5.3.1. Effective date

This policy is effective from January 1, 2024.

5.3.2. Transition period

NISCF's Certification Services requests made and NISCF's Certificate of Compliance issued, before the effective date of this policy are not subject to this policy until the Re-Certification stage.

Applicants to NISCF's Certification Services and holders of NISCF's Certificate of Compliance described in the previous paragraph can voluntarily conform with the statements defined in this policy before the Re-Certification stage.

5.4. Exceptions and deviations

5.4.1. Exceptions to Policy Statements

Exceptions to this policy shall only be defined by the National Cyber Security Agency (NCSA) through another policy and / or any NCSA's organizational structure that has been given the authority over the NISCF or the Certification Services.

5.4.2. Deviation process from Policy Statements

Deviation from policy statements shall be formally authorized in writing by the National Cyber Security Agency (NCSA).

5.4.3. Sanctions

National Cyber Security Agency (NCSA) reserves the right to not accept NISCF Certification Services requests and / or suspend or withdraw NISCF's Certificate of Compliance or any other Certificates, Credentials or Licenses provided by NCSA from

NISCF's Certification Services stakeholders that do not conform with the statements defined in this policy.

National Cyber Security Agency (NCSA) reserves the right to impose any monetary or procedural sanctions in virtue of the authority that has been granted to NCSA, though laws and regulations, on NISCF's Certification Services stakeholders that do not conform with the statements defined in this policy.

6. Annexes

6.1. Acronyms

AAEEBs	Audit, Assessment, Evaluation and Examination Bodies.
NCGAA	National Cyber Governance and Assurance Affairs.
NCSA	National Cyber Security Agency.
NISCF	National Information Security Compliance Framework.

6.2. Reference

Emiri Decree No 1 of year 2021.

President of National Cyber Security Agency (NCSA) Decision No 3 of year 2022.

NCSA-NISCF-CERT-GTXD (General Taxonomy Document for National Certification - Public).

End of Document