Cyber Security Policy of the Fiscal Information Agency and Regional National Taxation Bureaus

Version 2.6

February 4, 2025

Table of Revision Records

Version	Revision Date	Reference of Revision and Summary	Revised Page	Reviser
1.0	101.10.5	According to the 1st conference resolution from the information security committee (ISC) report		Executive Team of ISC
1.1	102.1.4	1. According to the 2nd conference resolution from the information security committee (ISC) report. The revised scope was extended to the information operation team of the Fiscal Information Agency 2. Updated organization name	all	Executive Team of ISC
1.2	104.3.4	6.3.1 Added “or re-evaluated when there are major changes in the organization…”	P.2	Executive Team of ISC
2.0	104.4.28	According to the resolution of the 2nd conference resolution from the information security committee (ISC) and audit team in 2015, in response to the release of a new version of the applicability statement, all ISMS common documents were updated	all	Executive Team of ISC
2.1	106.8.16	According to the resolution of the 2nd conference resolution from the information security committee (ISC) in 2017, following the expansion of the verification scope of the Fiscal Information Agency to the whole center, relevant regulations were added	P.1	Executive Team of ISC
2.2	107.7.26	According to the resolution of the 2nd conference resolution from the information security committee (ISC) in 2018, added the “Cyber Security Management Act” and 6. Information Security Declaration	P.1-2	Executive Team of ISC
2.3	108.9.17	According to the resolution of the 2nd conference resolution from the information security committee (ISC) in 2019,following the revision of the “Cyber Security Management Act”, deleted the “Information Security Declaration” and added “Concept”	all	Executive Team of ISC
2.4	109.8.21	According to the resolution of the 1st conference resolution from the information security committee (ISC) in 2020, following the revision of the related Cyber Security Management Directions for the MOF and Its Subordinate Agencies and the revision of the “Cyber Security Management Act”	all	Executive Team of ISC

2.5	111.3.28	Final approved by the chairperson of the Information Security Committee (ISC)- the related content in 1. is deleted due to the termination of two documents, "Information Security Management Directions for the Executive Yuan and its Subordinate Agencies" and "Information Security Management Guidelines of the Executive Yuan and Its Subordinate Agencies", which is terminated by Executive Yuan and National Development Council.	P.2	Executive Team of ISC
2.6	114.2.4	Approved by the members of the Cyber Security Committee and according to the resolutions of the 1st meeting of the Fiscal Information Agency Cyber Security and Personal Data Management Review Committee in 2025-Revised based on the renaming of the document titled "Basic Knowledge of Cyber Security of the Ministry of Finance and Its Subordinate Agencies".	P.5	Executive Team of ISC

1. References

1.1 “Cyber Security Management Act” and Related Regulations
1.2 “Cyber Security Policy and Organization Management Guidelines of the Ministry of Finance and Its Subordinate Agencies” promulgated by the Ministry of Finance
1.3 ISO27001 and CNS27001 Standards

2. Concept

The main idea of this cyber security policy is “Cyber Security is Everyone's Responsibility”. Colleagues shall be familiar with and follow cyber security regulations and the “Basic Knowledge of Cyber Security of the Ministry of Finance and Its Subordinate Agencies”, and implement the security protection of the information and communication devices and systems to ensure the information security of the organization.

3. Objectives

3.1 This policy is established to be the core guidance of the information security management system, for providing reliable information and communication services, assuring the confidentiality, integrity and availability of information, and complying with the “Cyber Security Management Act”, “Tax Collection Act”, “Regulations Governing the Use of Uniform Invoices”, “The Act Governing Local Tax Regulations”, “The Classified National Security Information Protection Act”, “Personal Data Protection Act” and other related regulations, to ensure the regularity, safety, and stability of the information and communication operations of the Fiscal Information Agency (including Service Support Division) and National Taxation Bureau of each region (the “Administrative Agencies”).

3.2 To effectively maintain the continuous operation of the administrative agencies effectively and reduce the risks associated with information and communication operations to achieve the objectives of "Implementing customer-oriented services and creating high quality lives" and "Optimizing resource allocation and improving the efficiency of tax administration".

4. Scope

4.1 The scope of the information security management systems covers the information and communication operations of the administrative agencies.

4.2 This policy applies to colleagues of the administrative agencies (including full-time employees, contractors, technicians, maintenance workers, temporary personnel, and part-time employees), business-related agencies (organizations), vendors, service providers and third-party personnel.

5. Accountability

5.1 Cyber Security Management Review Committee

The highest decision-making organization of the cyber security management of the administrative agencies; executing management review of general cybersecurity-related affairs.

5.2 Cyber Security Execution Team

Performing general asset risk assessment and risk management; revising and controlling the information security management system; performing business continuity management in information and communication operations.

5.3 Cyber Security Audit Team

Performing general cyber security audit.

5.4 Applicable personnel of this policy

Cooperating with the information security management system activities and abiding by relevant regulations.

6. Definitions

6.1 Cyber Security

Refers to such effort to prevent information and communication system or information from unauthorized access, use, control, disclosure, damage, alteration, destruction or other infringement to assure the confidentiality, integrity and availability of information and system.

6.2 Asset

Anything valuable to the organization, such as information, people, software, hardware, services, buildings, and protection facilities.

6.3 Cyber Security Management System

Information Security Management System (ISMS).

7. Implementation Guidelines

7.1 Principles

7.1.1 Consider relevant laws, regulations, and operational requirements, conduct asset risk assessments, confirm the security requirements of information and communication operations, establish standard operating procedures, adopt appropriate security control measures, to ensure asset security.

7.1.2 Establish a cyber security organization and determine the segregation of duties, to facilitate cyber security works.
7.1.3 Based on the roles and functions of personnel, establish an evaluation or assessment system, and conduct cyber security training as needed.
7.1.4 The provisions of asset access shall be based on business requirements and consider minimum permissions, segregation of duties and responsibilities, and independent review.
7.1.5 Establish cyber security incident management procedures to ensure a proper response, control and processing of incidents.
7.1.6 Develop a business continuity plan and conduct regular drills to ensure the continuity of information and communication operations.
7.1.7 According to the "Personal Data Protection Act", intellectual property rights, and relevant regulations, process and protect personal data and intellectual property rights prudently.
7.1.8 Conduct regular cybersecurity audits and review the implementation of the information security management system.
7.1.9 If colleagues of the administrative agencies violate this policy and the relevant cyber security regulations, they shall be dealt with the Reward and Punishment Regulations for Tax Officers of the Ministry of Finance or relevant regulations. Violations of relevant cyber security regulations by other personnel shall also be investigated for criminal responsibility following relevant laws and regulations.
7.2 Security Objectives
7.2.1 To maintain the continuity of information and communication operations of the administrative agencies to provide an integrated service across tax categories, agencies, and years.
7.2.2 To protect the assets related to the information and communication operation maintenance and management of the administrative agencies from improper or illegal use by human intent; to prevent the incursive and destructive behaviors by hackers and viruses.
7.2.3 To establish the information security management process and related standard operating procedures of the administrative agencies to avoid negligent behaviors and incidents, strengthen colleagues' cyber security awareness, and help to achieve the aim which collection of taxes and services could operate on a secure and integrated resource sharing platform.
7.3 Review
7.3.1 This policy shall be evaluated at least once a year, or re-evaluated when there are major changes in the organization (such as organizational adjustments, major system changes) to comply with the relevant regulations, latest technologies, and business operations of the administrative agencies, and shall be appropriately revised.
7.3.2 This policy is approved by the Cyber Security Management Review Committee and implemented on the announcement day, and the applicable personnel of this policy are notified in writing, electronically or in other ways.