

# Information Security and Cyber Security

## Policy

We recognize that it is our duty to protect the information assets entrusted to us by our customers and business partners as well as our own information assets in order to provide better products and services and contribute to the development of society. Based on this concept, NEC has positioned security, accurately referring to both information security and cyber security, as one of the critical subjects of “materiality,” its priority management theme from an ESG perspective—materiality, and has established its “Information Security Statement” as the basis for driving our efforts.

NEC has evaluated risks from various perspectives including the need of countermeasures as well as the possible damage both to corporate business and society, and has selected priority risks that will have huge impacts and that need to be addressed. With these risks in mind, we are deploying measures to counter cyber attacks that are becoming increasingly sophisticated, while complying with the U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework Version 1.1 and the Cybersecurity Management Guidelines Version 2.0 by Japan’s Ministry of Economy, Trade and Industry (METI).

In addition, almost 100% of our business divisions in which information security is particularly important, such as healthcare, finance, government, and cloud computing services, have obtained Information Security Management System (ISMS) certification.


Based on our information security implementation framework (see the figure below) as well as on our Purpose that shows why as a company we conduct business, NEC is working to realize a secure information society and provide value to our customers.

To protect information assets, NEC is taking the following approach:

- Implementing cyber attack measures
- Providing secure products, systems, and services
- Promoting information security in collaboration with business partners

At the same time, we have positioned information security management, information security infrastructure, and information security personnel as the three pillars of the information security governance framework within the NEC Group, thereby maintaining and improving our comprehensive and multilayered information security.

 NEC Information Security Statement

 Information Security Report

 Priority Management Themes from an ESG Perspective—Materiality

## Information Security Implementation Framework

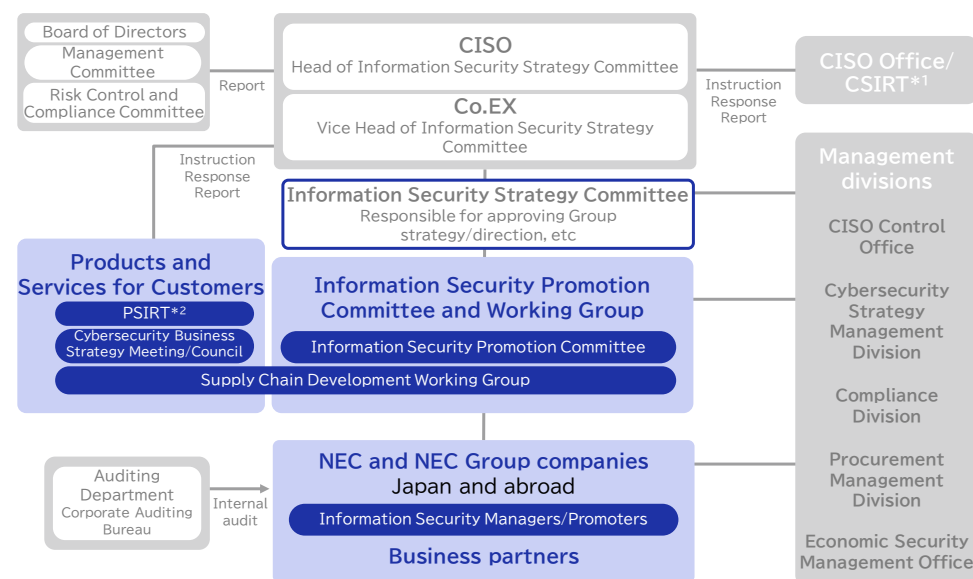


## Implementation Framework

The NEC Group’s information security implementation framework comprises the Information Security Strategy Committee, its subordinate organizations, and the people in charge of information security management and promotion at each Group company. Under the direction of the Chief Information Security Officer (CISO), the NEC Group devises information security measures based on cybersecurity analysis, and NEC Group companies cooperate to promote these measures. In addition, we conduct annual penetration tests via a third-party organization in order to assess vulnerability risks. We also conduct regular audits of all Internet servers four times a year. These actions ensure that vulnerabilities are dealt with in a timely manner. The corporate executive who assists the CISO oversees the office of the CISO, which promotes information security measures, and the PSIRT, which monitors for cyberattacks and resolves incidents quickly whenever they occur.

In light of recent geopolitical conditions, we have established the Economic Security Management Office. The office investigates and analyzes across the NEC Group cybersecurity, export restrictions, and other risks from an economic perspective, formulates strategies, and addresses these risks.

### The NEC Group’s Information Security Implementation Framework



\*1 Computer Security Incident Response Team

\*2 Product Security Incident Response Team

## Measures and Main Fiscal 2022 Activities

### Information Security Management

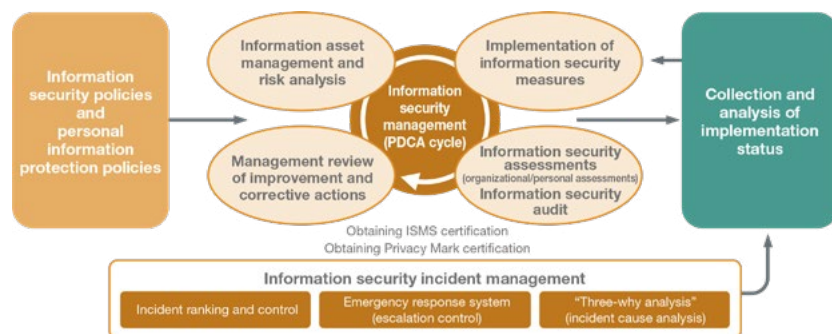
To facilitate the establishment of a variety of Group-wide measures, we have introduced an information security management system and security policy, both of which we make every effort to maintain and improve.

### Information Security Risk Assessment

The NEC Group conducts risk assessments and implements countermeasures by analyzing deviations from baseline criteria and carrying out detailed risk analysis, with both methods conducted in a proper manner. First, we ensure that security is implemented in line with criteria that serve as a baseline, and when more advanced management is necessary, we conduct a detailed risk analysis based on the Information Security Risk Assessment Criteria and implement finely tuned countermeasures.

### Risk Management for Information Security Incidents

Information security incidents are subject to mandatory reporting. The contents of these reports are analyzed and the results are put through a PDCA cycle for risk management assessment. Incident information is centrally managed for the entire NEC Group, and changes in the number of incidents, trends by organization and type of incident, and other data are analyzed. From there, NEC reflects this analysis in Group-wide measures while also measuring the impact of these incidents.



### Measures against Cyber Attacks

As cyber attacks grow increasingly complex and sophisticated, the NEC Group focuses on the protection of information assets entrusted by customers and business partners as well as its own. To this end, we have implemented total cyber security management by conducting uniform and advanced measures worldwide based on cyber security analysis, and established an incident response framework with our Computer Security Incident Response Team (CSIRT).

In particular, given that NEC creates and provides social solutions for countries worldwide, a single information security incident caused by a cyber attack or any other factor could diminish the social trust of the entire NEC Group and materially affect its business management. For this reason, we view a comprehensive and global approach to cyber security risks as essential for our business continuity.

We are strengthening our global measures against increasingly sophisticated cyber attacks based on a multilayered defense approach. In fiscal 2021, our measures focused on the following tasks.

Cyber risk assessments by “Red Team”	<ul style="list-style-type: none"> <li>The NEC Group utilizes “Red Team” to conduct regular cyber risk assessments with the aim of improving cyber resilience and accountability.</li> <li>Red Team conducts a global assessment consisting of three investigations on 1) the management status of critical information, 2) risks that allow us to perform a three-pronged investigation into management of important information and that include public server vulnerabilities and data leakage, and 3) internal and external security breaches from an attacker’s point of view. We can then make a global assessment, identify security risks we overlooked in our security measures and operations, and take actions for implementing improvements.</li> <li>We employ audit organizations and security specialists to conduct third-party attack diagnoses.</li> </ul>
Generating and utilizing threat intelligence	<ul style="list-style-type: none"> <li>Our team of Cyber Threat Intelligence specialists possesses an understanding of the threats facing NEC, detects their early signs as well as their precursors, and implements advanced proactive defense measures.</li> <li>The NEC Group conducts hunts for threats by using Group-wide endpoint detection and response (EDR) tools deployed across the Group and an integrated log analysis platform.</li> <li>We have also built up an investigation environment aimed at enhancing our active and unique CTI generation efforts, in addition to detailed threat analysis.</li> </ul>
Enhancing organizational security resilience	<ul style="list-style-type: none"> <li>We conduct training that addresses targeted email attacks to ensure that employees are prepared for ransomware and other global threats.</li> <li>We have developed a manual that provides the basis for comprehensive training exercises to ensure a rapid response if a ransomware attack occurs.</li> <li>Relevant departments and specialists hold training exercises at least every six months in preparation of a security incident.</li> <li>A third party evaluates the resilience of important systems to ensure high-level business continuity.</li> </ul>
Critical information management	<ul style="list-style-type: none"> <li>To minimize the impact of information leaks, we have defined “critical information” as information that would have a huge impact on our business management and performance if stolen or exposed externally.</li> <li>We have established a scheme for storing and handling critical information according to its importance, and are committed to taking stringent information management and countermeasures.</li> </ul>

Information Security Report

### Providing Secure Products, Systems, and Services

NEC has established a security implementation organization structure to facilitate secure development and operations of the products, systems, and services it provides to customers. This structure comprises information security managers assigned to each business unit and follows the concept of security by design (SBD) to ensure security comprehensively from the planning phase through to the operation phase.

Information Security Report

### Information Security in Collaboration with Business Partners

NEC conducts its business activities in collaboration with business partners. In these collaborations, we believe it is important to ensure that the technology capabilities and information security level of the business partners meet our required standards. To this end, NEC categorizes its business partners by information security level based on the implementation status of their information security measures. In selecting business partners for a project appropriately, we check the information security level to outsource tasks, thus reducing risks of information security incidents occurring at business partners. In addition to the measures stated above, we conduct document security survey checks and on-site inspections for business partners. Every year we review inspection items in light of any incident trends or in consideration of the business partner, issue a report of the inspection results and provide the business partner with feedback, and follow up on any issues that require improvement.

Information Security Report