

# Personal Information Protection and Privacy

## Policy

The NEC Group Code of Conduct stipulates respect for human rights and privacy and the management of personal information, and NEC has positioned “Provision and Utilization of AI with Respect for Human Rights (AI and Human Rights),” including personal information protection initiatives, as a priority management theme from an ESG perspective—materiality. From this perspective, we are tackling prevention of any privacy-related issues stemming from the handling of personal information in addition to undertaking other personal information protection measures.

### ■ Personal Information Protection

In October 2005, NEC Corporation received “PrivacyMark” certification, recognizing it as a business operator with systems in place to ensure appropriate protection measures for personal information in conformance with Japanese industrial standard JIS Q 15001 (personal information protection management systems—requirements). Since receiving the certification, we have stipulated within the NEC Privacy Policy that personal information must be handled in accordance with JIS Q 15001 standards.

In cooperation with its consolidated subsidiaries in Japan and overseas, NEC Corporation has also built an implementation framework for personal information protection and a personal information protection management system in compliance with the Act on the Protection of Personal Information and JIS Q 15001. Our personal information protection management system includes the establishment of data protection standards (personal data safety management measures and so on). Further, we conclude agreements with third parties with which we share data or outsource the handling of data requiring compliance with these standards. Also, we have established escalation rules and emergency response procedures to be followed in the event of incidents such as personal information leaks or mishandling of data.


### ■ Privacy

The General Data Protection Regulation (GDPR), which became effective in 2018 in the Europe Economic Area, is one example of the privacy protection laws and regulations currently being established in several countries and regions. As enforcement of these laws and regulations become more stringent, the roles and responsibilities placed on companies to protect privacy are increasing.


NEC Corporation aims to maximize social value and minimize the negative impact on society by developing and providing products and services with consideration for privacy issues, which may be perceived differently depending on the country, region or culture, and also with consideration for discrimination and other human rights issues that could be exacerbated with the use of AI. To clarify our stance, the NEC Group Code of Conduct stipulates that business activities aimed at resolving social issues using ICT must not give rise to human rights issues, including invasion of privacy.

NEC Corporation acquired PrivacyMark certification in October 2005 and subsequently renewed it for the ninth time in October 2021. As of the end of March 2022, NEC Corporation and its 31 affiliated companies have obtained this certification. In principle, we forbid acquiring information that could have an economic impact such as bank account or credit card numbers, sensitive information such as one’s birthplace, or highly private information such as mobile telephone numbers without the principal’s prior consent.

 **Topic: Respecting Human Rights**

 **AI and Human Rights**

 NEC Privacy Policy

 NEC Group AI and Human Rights Principles



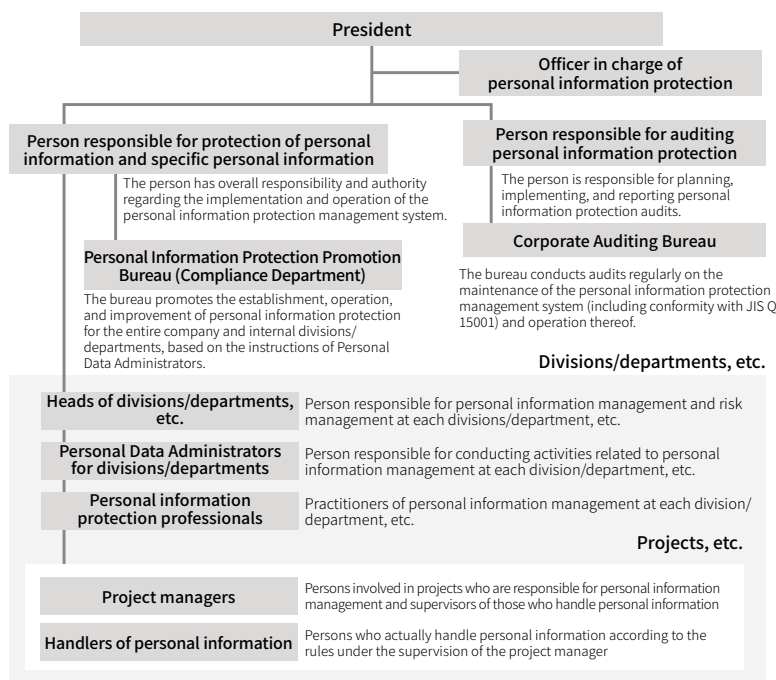
## Implementation Framework

At NEC Corporation, the head of the department responsible for protecting personal information serves as the Personal Information Protection Administrator, the person in charge of implementing the personal information protection management system. This person is responsible for protecting specific personal information with respect to the Social Security and Tax Number System as well.

The Compliance Department plays a central part in promoting the protection of personal information within the NEC Group under the leadership of the head of the Personal Information Protection Promotion Bureau appointed by the Personal Information Protection Administrator.

In addition, we conduct regular audits of privacy protection in conformance with JIS Q 15001, with the General Manager of the Corporate Auditing Bureau serving as Chief Personal Information Protection Auditor.

The general managers are responsible for managing personal information protection in their respective divisions. Each appoints a division personal information protection manager, who is responsible for carrying out personal information protection management for the division, and a personal information protection professional, who possesses expert insight regarding the protection of the personal information protection management system by inspecting personal information, including human rights and privacy issues, and through personal information handling in each division and improving handling rules based on the inspection results. The person responsible for handling personal information for each project ensures that persons who handle personal information undertake thorough personal information protection measures.

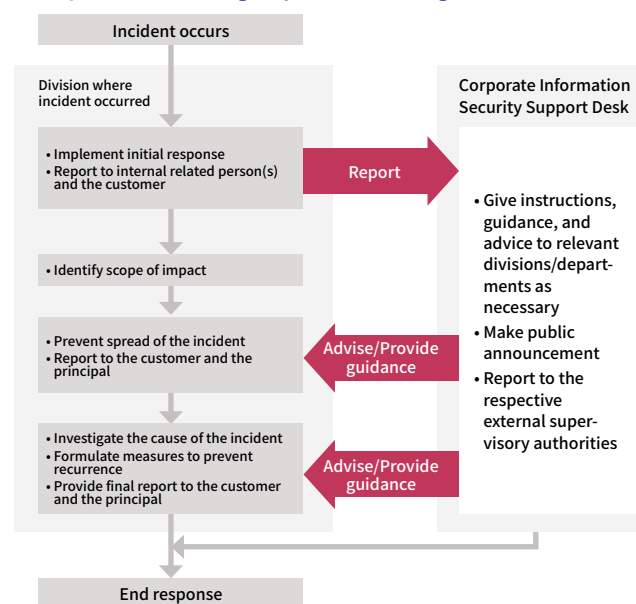


## Consolidated Subsidiary Management Framework

At our consolidated subsidiaries in Japan, we have built systems to comply with the Act on the Protection of Personal Information and the Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures, the so-called My Number Act, which is related to the numbers used to identify individual residents of Japan for administrative procedures, and we use these systems to promote the protection of personal information. Furthermore, 30 consolidated subsidiaries in Japan have acquired PrivacyMark certification as of March 31, 2022.

At our consolidated overseas subsidiaries, we are tackling compliance with the laws and regulations in each jurisdiction as a matter of course, and we have appointed a Personal Data Administrator at each of our major subsidiaries to promote the protection of personal information.

## Response in an Emergency Such as Leakage of Personal Information



NEC maintains systems for responding swiftly if an incident occurs involving the loss, outflow or leak, etc., of personal information. If an incident should occur, the response is coordinated quickly and systematically based on standardized procedures. Specifically, if an incident occurs related to personal information or an event takes place for which the occurrence of such an incident is a possibility, the discoverer or the employee involved in the incident contacts their manager and the NEC Group contact window for information security incidents. The person at the contact window then coordinates the necessary response with the related divisions that make up the Personal Information Protection Promotion Bureau and relevant divisions in accordance with applicable laws, ordinances, ministry guidelines, and other regulations, taking into account the risk for infringing on the rights and interests of the persons

involved. These responses may include promptly notifying the people concerned, making a public announcement, and taking corrective measures appropriate to the incident.

## Response to Requests from National Governments for Personal Information Provision

If NEC Corporation's business divisions are requested by a government or law enforcement agency of a country to provide personal information that the Company holds, the general manager of the division that receives the request reports to and consults with the Personal Information Protection Administrator as necessary. In such cases, the Personal Information Protection Administrator reports to and consults with the executive officer in charge of personal information protection and management. Premised upon respect for the human rights of the person in question, the Company will then determine the necessity of providing such information and undertake the appropriate procedures and measures pursuant to the applicable laws.

## Measures and Main Fiscal 2022 Activities

### ■ Personal Information Protection Training

Training for all officers and employees (NEC Corporation)	<ul style="list-style-type: none"> <li>The Company conducts web-based information security training once a year. (Completion rate of Companywide training in fiscal 2022: 98%)</li> </ul>
Education for personal information protection professionals (NEC Corporation, all business units)	<ul style="list-style-type: none"> <li>Textbooks have been prepared on risk management in the handling of personal information, in addition to education through 16 classroom lectures.</li> <li>Practical education through three assignments that must be submitted</li> <li>Courses aimed at acquiring personal information protection qualifications</li> <li>Human rights and privacy education</li> <li>Education related to the Act on the Protection of Personal Information, amended in 2020</li> <li>Lectures by an external lawyer</li> <li>Course for dealing with the Act in practice (held eight times)</li> </ul>
Training for newly hired employees and transferred employees (NEC Corporation and its consolidated subsidiaries in Japan)	<ul style="list-style-type: none"> <li>Created a textbook on personal information protection as an introductory training material; used textbook to train newly hired and transferred employees</li> <li>When there is a request from a division/department, or when it is otherwise deemed necessary by the Personal Information Protection Promotion Bureau, awareness training is conducted as appropriate at business units or consolidated subsidiaries in Japan.</li> </ul>

### ■ Management of Personal Information

Initiatives at NEC Corporation	<ul style="list-style-type: none"> <li>NEC Corporation runs the Personal Identifiable Information Control System, a ledger-based system to manage personal information and make its management more transparent.</li> <li>We have documented standard procedures and operate a personal information protection management system. Also, as necessary, operational rules are created at the division level and by type of personal information and are rigorously enforced.</li> <li>To raise awareness of personal information protection and information security in general, the Basic Rules for Handling Customer-related Work and Trade Secrets have been established, and NEC Corporation rigorously informs all employees about these rules.</li> <li>In fiscal 2021, there were no incidents involving the loss, outflow or leak, etc., of personal information at NEC as a result of the above efforts.</li> <li>There were no complaints from the Ministry of Economy, Trade and Industry, which oversees the industrial area where NEC operates, the Personal Information Protection Commission, or from any other third-party institutions about customer privacy breach or other issues.</li> </ul>
Initiatives for customers and business partners	<ul style="list-style-type: none"> <li>NEC Corporation and its consolidated subsidiaries in Japan establish data protection standards (personal data safety management measures and so on) for contractors that handle personal information, conclude agreements with contractors with which data is shared requiring compliance with these standards, and require contractors to conduct privacy management equivalent to that of the NEC Group.</li> <li>We request the contractors engaged in work for NEC Corporation or its consolidated subsidiaries in Japan to submit a pledge on the Basic Rules for Customer-Related Work and to have their employees take an online test to verify their knowledge. These steps help ensure rigorous management of personal information.</li> <li>In fiscal 2021, there were no incidents involving the loss, outflow or leak, etc., of personal information as a result of the above efforts.</li> <li>We make sure to handle "My Number" data carefully and securely since it is Specific Personal Information. We are carrying out initiatives to deploy technical measures to ensure secure operations by controlling access, blocking unauthorized external access, and preventing information leaks, etc., while maintaining sufficient privacy protection levels in each system.</li> </ul>

 Information Security and Cyber Security

#### Personal information management initiatives abroad

- We appoint Personal Data Administrators at our consolidated overseas subsidiaries to maintain a global management framework. At the same time, we create personal information management ledgers at each subsidiary to have an understanding of the information being handled by each company and the risks involved. We also work to ensure that the procedures to manage these risks as well as common safety measures that need to be observed are disseminated thoroughly.
- We also ensure that consolidated overseas subsidiaries implement personal information management rules that comply with personal information protection laws and regulations in the country or region in question as well as any applicable laws and regulations from outside the country or region in question. In addition, NEC Group companies obtain the principal's consent and enter into any required data transfer contracts based on the laws and regulations in each country or region to facilitate any cross-border transfer of personal information for employees or otherwise.

### ■ Monitoring and Improvement

NEC Corporation appropriately manages personal information by executing plan-do-check-act (PDCA) cycles on an autonomous basis through various inspection activities.

Also, NEC Corporation and its consolidated subsidiaries in Japan conduct regular internal audits based on internal audit check items stipulated in JIS Q 15001. Further, for operations related to the handling of "My Number" data, we use security control measure check sheets prepared based on Japan's security control regulations and self-check sheets during re-entrustment in order to monitor divisions and subcontractors handling "My Number" data.

#### Verification of the operation of information security measures

- The implementation of security measures carried out by all employees is verified once a year. If there are cases of non-compliance, improvement plans are formulated and carried out at the organization level.

#### Verification of the status of personal information management

- Control forms registered in the Personal Identifiable Information Control System are reviewed at least once a year to validate the status of information management.
- In addition, once a year the general managers of each business unit implement management reviews to confirm the status of personal information management to allow for corrective action to be taken when needed, and to maintain appropriate management conditions.

#### Verification of operations during emergencies

- Operation of the above information security measures is thoroughly reviewed as the need arises, in the event of an incident involving the loss, outflow or leak, etc., of personal information.