

Sustainable Management	Environment	Governance	Social	67-70 Inclusion and Diversity 71-74 Human Resources Development and Training 75-76 Creating a Diverse Work Style Environment	77-79 Health and Safety 80 AI and Human Rights 81-83 Personal Information Protection and Privacy	84-86 Information Security and Cyber Security 87-88 Ensuring Quality and Safety 89 CS (Customer Satisfaction) Initiative	90-91 Cooperation with the Local Communities
------------------------	-------------	------------	---------------	--	---	--	--

Personal Information Protection and Privacy

Policy

Rapid progress and spread of the internet and ICT have driven a swift expansion in ownership of electronic devices such as smartphones. In addition, with progress in the creation of new services and innovations using AI, the need to protect personal information and privacy has become an even greater concern. Especially in Europe, the Charter of Fundamental Rights of the European Union stipulates protection of personal information as a fundamental right requiring protection. The EU's General Data Protection Regulation (GDPR), which became effective in May 2018, stipulates methods of protection and management of personal information to protect and establish personal information and privacy rights.

Failure to consider these issues would be a serious risk for the Company as it seeks to provide social values such as safety, security, fairness, and efficiency through our services and solutions. On the other hand, by providing services and solutions that consider these issues we believe we can provide highly reliable value to society, including our customers.

The NEC Group Code of Conduct stipulates the management of confidential information and personal information, and NEC has positioned personal information protection initiatives and "Privacy policies and measures aligned with social receptivity" as themes of priority management "materiality" from an ESG perspective.

We have studied the trends related to this framework of new laws and regulations, and we are addressing these problems regarding personal information protection or privacy by following the policies described below.

<Personal Information Protection>

Personal information refers to personally identifiable information, which includes numbers and other identifiers and we recognize that appropriately protecting personal numbers and other personal information received from shareholders, investors, business partners, employees and others is one of our social responsibilities. We have implemented and maintain the NEC Privacy Policy, which stipulates that personal information must be handled in conformance with Japan's Act on the Protection of Personal Information and JIS Q 15001 (Personal information protection management systems - requirements), the Japanese industrial standard for safe and appropriate management of personal information handled by

corporations and other organizations in the course of their operations. In the event that the Company's policy should change, we will promptly give notice on the Company's public website and to all of our employees, in accordance with JIS Q 15001.

▶ [NEC Privacy Policy](#)

In cooperation with its consolidated subsidiaries throughout the world, NEC Corporation has built a system for promoting privacy 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 emergency response procedures for incidents such as personal information leaks.

<Privacy>

NEC Corporation acquired "Privacy Mark" certification in October 2005 and subsequently renewed it in October 2019. The Privacy Mark is conferred on companies that comply with JIS Q 15001 and are recognized by a third-party organization as having systems in place to ensure appropriate protection measures for personal information. As of the end of March 2020, NEC Corporation and its 29 affiliated companies have obtained this certification. In principle, we forbid acquiring information that can have an economic impact such as bank account or credit card numbers, sensitive information such as birthplace, or highly private information such as mobile telephone numbers without, the person's consent.



As was the case with GDPR, privacy laws are being created as a global trend and the roles and responsibilities required of companies have been increasing. NEC Corporation aims to maximize social value as well as to minimize the negative impact on society by developing and providing products and services that consider privacy issues, which can be perceived differently depending on country, region or culture, and human rights issues such as discrimination that may be aggravated by leveraging AI.

To clarify our stance, in April 2019, we formulated and announced the "NEC Group AI and Human Rights Principles." The Companywide principles will guide our employees to recognize respect for human rights as the highest priority in each and every stage of our business operations in relation to social implementation of AI and utilization of biometrics and other data (hereinafter referred to as "AI utilization") and enable them to take action accordingly.

In addition, the NEC Group Code of Conduct also stipulates that business activities aimed at solving social issues by using ICT must not give rise to human rights issues, including invasion of privacy.

- ▶ [NEC Group AI and Human Rights Principles](#)
- ▶ [Respect for Human Rights](#)
- ▶ [AI and Human Rights](#)

Sustainable Management	Environment	Governance	Social	67-70 Inclusion and Diversity 71-74 Human Resources Development and Training 75-76 Creating a Diverse Work Style Environment	77-79 Health and Safety 80 AI and Human Rights 81-83 Personal Information Protection and Privacy	84-86 Information Security and Cyber Security 87-88 Ensuring Quality and Safety 89 CS (Customer Satisfaction) Initiative	90-91 Cooperation with the Local Communities
------------------------	-------------	------------	---------------	--	---	--	--

Promotion Framework

At NEC Corporation, the head of the responsible division for protecting personal information serves as the "Personal Information Protection Administrator," the person in charge of implementing the personal information protection management system. Further, we have added the role of protecting specific information with respect to the Social Security and Tax Number System to the duties of the Personal Information Protection Administrator.

The Customer Information Security Office of the Compliance Division 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 protection of personal information. The manager operates a personal information protection management system by inspecting personal information protection risk management and 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 domestic consolidated subsidiaries, we have built systems to comply with the Act on the Protection of Personal Information and the so-called Individual Number Act, which is designed to centrally manage information related to social security and tax by assigning a number to individual citizens of Japan.

At our overseas consolidated subsidiaries, we naturally comply with the laws in each country, and we have appointed a Personal Data Administrator at each of our

major overseas subsidiaries to promote protection of personal information.

Emergency Response to Information Leaks

The NEC Group maintains systems following JIS Q 15001 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 there is such risk, the discoverer or the employee involved in the incident contacts his or her manager and the NEC Group contact window for information security incidents. The person at that contact window then coordinates the necessary response with the related divisions that make up the Personal Information Protection 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 in Other Countries to Provide Personal Information

If NEC Corporation's business divisions are requested by the governments of other countries to provide personal information, the general manager of the division that receives the request is responsible for responding. If necessary, the general manager may report and consult with the Personal Information Protection Administrator, and the Administrator may report and consult with the executive officer in charge of personal information protection and management. The general manager of the business division confirms the requesting party's objective for using the information, then decides whether or not to provide the information following the laws and regulations of the country concerned. In providing the information, the general rule is to obtain consent from the information owner and keep a record of its provision. However, there are cases where consent is not obtained pursuant to the laws and regulations of that country, or when no record is kept of its provision. Considering the purpose behind the establishment of the laws and regulations in each country,

NEC does not publicly announce the number of cases of such government requests.

Sustainable Management	Environment	Governance	Social	67-70 Inclusion and Diversity 71-74 Human Resources Development and Training 75-76 Creating a Diverse Work Style Environment	77-79 Health and Safety 80 AI and Human Rights 81-83 Personal Information Protection and Privacy	84-86 Information Security and Cyber Security 87-88 Ensuring Quality and Safety 89 CS (Customer Satisfaction) Initiative	90-91 Cooperation with the Local Communities
------------------------	-------------	------------	---------------	--	---	--	--

Main Activities and Results for Fiscal 2020

Training for Personal Information Protection

NEC Corporation conducts the following training for each management level in the organization.

1. Training for all officers and employees of NEC Corporation
Online training on information security, including aspects of personal information protection, is held online once a year for officers and employees of NEC Corporation. In fiscal 2020, the completion rate was 98%.
2. Training for personal information protection promoters for NEC Corporation and its domestic subsidiaries
Group training for information security promoters involved in promoting personal information protection was held two times in fiscal 2020.
3. Training for newly hired employees and transferred employees of NEC Corporation and its domestic consolidated subsidiaries
In fiscal 2020, we created a textbook on personal information protection as introductory training material and used it in training of newly hired and transferred employees. Apart from this training, when there is a request from a business division, or when it is otherwise deemed necessary by the Personal Information Protection Bureau, awareness training is conducted as appropriate at divisions or domestic consolidated subsidiaries.

Management of Personal Information

Initiatives at NEC Corporation

NEC Corporation runs the "Personal Identifiable Information Control System," a ledger-based system to manage personal information and make its management more transparent.

Furthermore, 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 rigorously enforced.

In addition, in order 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 all NEC Corporation employees are encouraged to submit pledges.

As a result of these efforts, there were no incidents involving the loss, outflow or leak, etc., of personal information at NEC in fiscal 2020. There were also no complaints from the Ministry of Economy, Trade and Industry, which oversees the industrial area where NEC belongs, the Personal Information Protection Commission, or from any other third-party institutions about customer privacy breach or other issues.

Initiatives for Customers and Business Partners

NEC Corporation and its domestic consolidated subsidiaries request their contractors handling personal information to conduct privacy management equivalent to that of the NEC Group. Moreover, we request the contractors engaged in work for NEC Corporation or its domestic consolidated subsidiaries to submit a pledge on the "Basic Rules for Customer-Related Work" and to have their employees take a regular online test to verify their knowledge. These steps help ensure rigorous management of personal information. As a result of these efforts, in fiscal 2020 there were no incidents involving the loss, outflow or leak, etc., of personal information.

An "Individual Number" is Specific Personal Information that must be handled carefully, and we are doing so with security ensured. 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.

Information Security and Cyber Security

Personal Information Management Initiatives Overseas

Recently, countries around the world, such as in Europe, are making rigorous laws and regulations regarding personal information. In this situation, NEC is ensuring proper information management globally as it pursues worldwide development of personal information-related businesses, such as AI, big data, IoT, and facial authentication. We appoint Personal Data Administrators at our overseas consolidated subsidiaries to create a global management framework. At the same time, we are creating

personal information management ledgers at every company and ensuring that everyone understands the procedures for managing them and the common information security rules that need to be observed. With regard to GDPR, our consolidated subsidiaries in Japan and Europe have formulated personal information management rules based on the regulations and have concluded transfer agreements throughout the entire Group to ensure that cross-border transfer of personal information of European employees and others is conducted legally. In other areas, we have confirmed the legal and regulatory situation in relevant countries, such as the California Consumer Privacy Act (CCPA) and Thailand's Privacy Data Protection Act (PDPA), and we are making the necessary preparations to comply with them.

Monitoring and Improvement

NEC Corporation appropriately manages personal information by executing PDCA cycles on an autonomous basis through various inspection activities.

Also, NEC Corporation and its domestic consolidated subsidiaries conduct regular internal audits based on internal audit check items stipulated in JIS Q15001. Further, for operations related to handling of Individual Numbers, 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 Individual Numbers.

1. Verification of the operation of information security measures
At NEC Corporation, implementation of information security measures by individual employees is verified once a year, and if there are cases of non-compliance, improvement plans are formulated and carried out at the organization level.
2. Verification of status of personal information management
At NEC Corporation, control forms registered in the Personal Identifiable Information Control System are reviewed at least once a year to validate the status of management of the various types of personal information handled by each organization.
3. Verification of operations during emergencies
Operation of the above information security measures is thoroughly reviewed and readjusted as the need arises, in the event of an incident involving the loss, outflow or leak, etc., of personal information.