Information Security Report 2010
Year ended March 31, 2010

Information Security Supporting an Information Society Friendly to Humans and the Earth

NEC Corporation
# Contents

<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>NEC’s Approach to Information Security</td>
</tr>
<tr>
<td>02</td>
<td>Information Security Promotion Framework</td>
</tr>
<tr>
<td>03</td>
<td>Information Security Governance</td>
</tr>
<tr>
<td>04</td>
<td>Information Security Management</td>
</tr>
<tr>
<td>08</td>
<td>Information Security Platform</td>
</tr>
<tr>
<td>14</td>
<td>Information Security Human Resources Development</td>
</tr>
<tr>
<td>16</td>
<td>Information Security Measures in Cooperation with Suppliers</td>
</tr>
<tr>
<td>18</td>
<td>Improving the Security of Products and Services</td>
</tr>
<tr>
<td>20</td>
<td>Security Solutions Trusted by Customers</td>
</tr>
<tr>
<td>22</td>
<td>Third-Party Evaluation and Certification</td>
</tr>
<tr>
<td>24</td>
<td>Corporate Data</td>
</tr>
</tbody>
</table>

## On the Publication of This Report

This report is being published to provide a better understanding of information security initiatives in the NEC Group. The report covers related initiatives through March 2010.

For Inquiries Regarding This Report
- NEC Corporation
- Management Information Systems Division
- Security Technology Center
- NEC Headquarters
  - 7-1 Shiba 5-chome, Minato-ku, Tokyo 108-8001
  - Tel. 03-3798-6980
In 2008 the NEC Group pledged to become “a leading global company leveraging the power of innovation to realize an information society friendly to humans and the earth” as part of our NEC Group Vision 2017. We also systematized all of our management activities as The NEC Way. Under our V2012 Mid-Term Growth Plan, we aim to achieve NEC Group Vision 2017 through customer-driven solutions leveraging our competitive strengths. These strengths lie in the integration of IT and networks, in particular building on the trend toward cloud computing. But we will also continue to utilize the strengths we have accumulated over more than thirty years as leading practitioners of the integration of computers and communications (C&C). All of these strengths will enable us to expand our business globally under our “One NEC” concept and contribute to our customers and the future of society.

To carry out The NEC Way, we believe we must enforce compliance with relevant laws and regulations as a matter of course. But we must also enhance our corporate value as we fulfill our social responsibilities as a good corporate citizen, working to earn the trust of all stakeholders, including our customers, shareholders, other investors, suppliers, local communities, and employees. In fulfilling our social responsibilities, the NEC Group puts particularly strong emphasis on maintaining and enhancing information security. This is because improper access, leaks, alterations, losses, theft, destruction, and interference with the use of information assets cause substantial damage and inconveniences for society as a whole.

It has been ten years since the NEC Group first recognized information security as an important management issue and began considering it on a company-wide committee level. Today, our efforts are focused on the following five points:

- Ensuring that the NEC Group works together as “One NEC” to promote the maintenance and enhancement of information security.
- Expanding measures to include not just the NEC Group, but our suppliers as well.
- Achieving a balance between the appropriate protection of information and its appropriate sharing and use.
- Using a comprehensive approach that incorporates the building of information security management systems, and the establishment of information security platform, and the development of human resources for information security, all to maintain and enhance information security on multiple levels.
- Providing customers with reliable security solutions that have been proven in-house.

This report presents the NEC Group’s information security initiatives. Please use it to deepen your understanding of these important initiatives.
We are promoting measures across the NEC Group to protect the information assets entrusted to us by our customers and suppliers, to provide reliable products, services, and information security solutions, and to conduct appropriate reporting and information disclosure.

We must raise information security levels across the NEC Group to earn the trust of society. To achieve this, rather than promoting information security at the individual company level, we are building an information security governance system for the Group as a whole. This will ensure that the effectiveness and efficiency of these measures can be demonstrated by the entire Group.

Each of NEC’s business units and Group companies has established information management security systems based on company-wide standards, taking into consideration the business environment and internal systems of each organization. While striving to maintain consistency with Group-wide policies, each organization is working to establish, operate, review, and improve its policies. Information security management systems are broadly made up of the following three major policy areas:

- Information security management, which centers on the preparation of relevant rules and regulations, and a system for implementing PDCA cycles
- Information security platform centered on IT initiatives designed to protect networks, operation systems, PCs, and so forth from various threats
- Development of human resources for information security, including improved awareness of information security and enhanced practical capabilities

Various measures in each area are then combined in a comprehensive, multi-layered structure to maintain and enhance information security.

Additionally, information security policies for suppliers are unified on a Group-wide level to ensure that suppliers do not encounter difficulties in responding to instructions from multiple NEC Group companies.
Under the “One NEC” concept, the NEC Group is promoting information security together with Group management while strengthening governance to maintain and enhance the level of information security across the entire Group.

Approach to Information Security Governance

At the NEC Group, management systems have been built at the individual business-unit or each group company. And each organization is required to maintain and enhance its information security based on a PDCA cycle.

We believe it is important that each of these activities be implemented efficiently and effectively as “One NEC” while ensuring effective governance to enhance security levels across the Group. Specifically, NEC defines goals of information security levels in the Group and provides all organizations with the direction of principles on effective measures across the Group and on the allocation of business resources to achieve the goals. We also monitor and evaluate the status of information security including all incidents in the Group. Then we provide the organization with a guidance as necessary and make improvements from results of the evaluation.

NEC discloses the information on these activities through our Annual CSR Report and this Information Security Report to fulfill our accountability to stakeholders.

Overall Information Security System Integrated with Group Management

The Information Security Strategy Committee, chaired by a senior executive vice president, promotes the NEC Group’s Information Security Governance. It has three promotion committees for domestic and overseas subsidiaries and suppliers. These committees are responsible for explaining various measures, sharing information about incidents, and informing directions. The business division heads in each organization act as information security managers, with primary responsibility for information security in their divisions including at group companies under their jurisdiction. They designate management promotion staff from among their managerial ranks, ensure thorough dissemination of rules within their organizations, and are responsible for the implementation and execution of security measures. They review the status of execution and do necessary improvement. The NEC division with overall responsibility for information security also works closely with related head office staff divisions to move the concrete development of each measure forward.

In fiscal 2010, we established the NEC Group Management Policy, which is designed to achieve a global standard management foundation. And the Group moved ahead to standardize rules regarding the performance of business and to unify systems, business processes, and infrastructure.
We are implementing various information security measures throughout the NEC Group, and are working to strengthen information security through a PDCA cycle.

Information Security Management Structure

To ensure solid execution of our information security policies for the maintenance and enhancement of our information security, the NEC Group believes it is important to continuously implement a PDCA cycle. The cycle has four steps: 1) Plan: establish a system 2) Do: implement and operate it 3) Check: review and re-evaluate it 4) Act: maintain and improve the system.

Through each process, we work to establish and maintain policies, manage information security risks, roll out management measures, check and audit, and learn from any incidents that arise. We also have systems in place for obtaining Information Security Management System (ISMS) and Privacy Mark certification, and maintain an awareness of other third party security certification.

Information Security Policy

The NEC Group has positioned information security as key to the performance of our business. And we disclose NEC Information Security Statement to the public.

Moreover, in the information security segment of the NEC Group management policy we establish basic information security rules, rules for information management (corporate confidential information management rules, personal information protection rules, and technical document management rules), and IT security rules. In this manner, we are working hard to prepare and strengthen an environment in which all employees are able to align their efforts in a common direction and demonstrate the NEC Group’s collective strengths. The implementation of these management policies is nearly complete in Japan. The implementation to overseas is planned for completion in fiscal 2011.
In the NEC Group, the protection of personal information is positioned as an important part of our compliance activities. So we have continued to strive to reinforce personal information protection.

In July 2000, we established the NEC Privacy Policy. And in October 2005, NEC obtained Privacy Mark certification. Ever since, we have worked to protect personal information using management systems that are fully compliant with the Japan Industrial Standards Management System for the Protection of Personal Information (JIS Q 15001) and with Japan’s Personal Information Protection Law. 42 companies in the NEC Group had obtained Privacy Mark certification as of the end of March 2010. We have also begun creating common protection management levels across the Group.

Information Security Risk Management

The NEC Group has established a set of Information Security Measure Standards (ISO/IEC 27001 compliant). They maintain common information security levels to be implemented across the Group. And by checking the status of implementation, we maintain information security at appropriate levels. When more advanced management is required, we provide a system by which business divisions can analyze their individual business execution risks based on assessment standards.

In addition, escalation rules for information security incidents have been standardized, enabling more appropriate care and quicker resolution for our customers. Moreover, management of information about such incidents has been centralized across the Group. We analyze incident data and seek real causes so that similar incidents can be prevented. And we also use the results of analysis to maintain the PDCA cycle for Information Security Management.

(1) Macro Analysis
Macro analysis enables us to examine the number of incidents after implementation of information security measures and trends of incidents by type or by company (NEC, Group companies, suppliers, etc.). This analysis is reflected in the NEC Group information security policies.

(2) Implementing Three-Why Analysis
Three-Why Analysis is conducted based on a ranking of each incident to seek out the real causes of information security incidents. It is a process in which repeated “why” questions are asked to analyze the fundamental cause of a problem and formulate measures to prevent recurrence. The analysis method is standardized. And by having the division in question conduct its own analysis, it becomes possible to ensure that the resulting improvements are instituted as part of day-to-day operations.

In the case of particularly serious incidents, a specialist adviser will participate in a meeting for more in-depth analysis. Top management is notified of the results. We roll them out across the company and they are reflected in subsequent information security measures.
The NEC Group conducts information security assessment for ensuring that information security measures have been strictly implemented within each organization. We have conducted assessments twice a year since fiscal 2006, and established a PDCA cycle for security improvement activities.

Aiming to eliminate the occurrence of any security incidents that could be prevented if the information security assessment was implemented strictly, the fiscal 2010 assessment was conducted targeting 98 domestic companies and 87 overseas companies, 185 Group Companies in total (an increase in the companies subject to assessment compared with those in the previous year).

(1) Description of Information Security Assessment

Five priority measures were defined specifically aimed at eradicating information security incidents related to information leaks. As a result of incident analysis, these measures were determined as those reducing or eliminating the primary cause of the incidents. The measures include: 1) security measures for use of USB flash drives and other removable storage media 2) security measures for the work outside the company 3) assessment of personal information relating to priority measures 4) security measures for entry passes 5) confidential information management involved in an outsourcing business with partner companies.

(2) Method for Conducting Information Security Assessment

The information security assessment was conducted from the management (organizational assessment) and implementation (individual assessment) point of view. Then by reviewing the results of the gap analysis, we clarified the problems on both management and implementation sides. To cope with these problems, we established a PDCA cycle between the Information Security Promoters and the individual staff members in each organization, and between supervisors and their subordinates in pursuit of improved management activity at the working level.

(3) Improvements Made Through Utilization of Assessment Results

As a result of the assessment, each organization worked to understand the causes of an inadequately implemented security measure, make an action plan to improve the security level and carry out the plan. The organization made the Information Security Promotion Plan for fiscal 2011. And the plan included the insufficient security measures for fiscal 2010 and new security measures for fiscal 2011. As a result, the organization can keep following the PDCA cycle.

In fiscal 2011 the NEC Group plans to conduct the assessment by each employee role.
For those organizations which need to obtain ISMS certification, the NEC Group provides a system to support the obtainment and management of the certification. Specifically, services are centered on standard ISMS content, and include consultation, audit structure development, training, and effective assessment methods (differential assessments, etc.). Standard ISMS content is designed to completely meet portions required under ISO specifications. NEC Group Promotional Office added Group Policy to the content. It is also possible to add independent components of each organization to the content. Through support for the obtainment and management of ISMS certification, NEC has unified Group policies and is making use of best practices from organizations that have already obtained certification.

To date, this system has been used by 72 organizations throughout the NEC Group. The know-how that has been gained as a result is being provided as solutions (the NetSociety for ISMS service) to our customers and suppliers.

Information security audits center on NEC’s Corporate Auditing Bureau, which conducts ISMS and Privacy Mark-related audits. The Corporate Auditing Bureau conducts internal audits of each business division regularly, based on ISO/IEC 27001 and JIS Q 15001 audit standards.

Efforts to Obtain Information Security Management System (ISMS) Certification

For those organizations which need to obtain ISMS certification, the NEC Group provides a system to support the obtainment and management of the certification.

Specifically, services are centered on standard ISMS content, and include consultation, audit structure development, training, and effective assessment methods (differential assessments, etc.). Standard ISMS content is designed to completely meet portions required under ISO specifications. NEC Group Promotional Office added Group Policy to the content. It is also possible to add independent components of each organization to the content. Through support for the obtainment and management of ISMS certification, NEC has unified Group policies and is making use of best practices from organizations that have already obtained certification.

To date, this system has been used by 72 organizations throughout the NEC Group. The know-how that has been gained as a result is being provided as solutions (the NetSociety for ISMS service) to our customers and suppliers.
The NEC Group has built and operates an IT platform designed to protect customer and other confidential information, ensuring secure and efficient access to networks and business systems globally.

Information Security Features

Through the information security platform, NEC has achieved secure, efficient execution of NEC Group business operations, including our suppliers based on NEC Group information security policies.

To protect confidential information, such as customer information, measures are needed to prevent access to information by anyone without the need to know, and transport information outside the company. This can be managed by establishing rules and enacting behavioral measures, however, inadequate knowledge of the rules, a drop in operational efficiency, or other problems may occur. So, by building an IT system that enables secure access to, removal, and sharing of information, we ensure that even if information is taken outside, only those who have been granted the proper authority can access the information. Finally, we work to achieve a balance between security measures and business efficiency.

Information Security Architecture

The information security platform consists of three platforms, “IT platform for user management and control,” “IT platform for PC and network protection” and “IT platform for information protection.”

The “IT platform for user management and control” is the platform for authentication, realizing centralized management of all NEC Group employee and contract staff data and restricting access to systems and information based on authorization.

The “IT platform for PC and network protection” safeguards PCs and networks from viruses, worms, unauthorized access, and other threats, ensuring there is an environment in which employees can work securely anytime, anywhere.

Finally, the “IT platform for information protection” builds on the above systems to protect the information. It provides encryption and other systems to prevent information leak. It also provides a secure environment for sharing information with suppliers.
Authentication systems are the foundation of information security management. The NEC Group built a system to identify individuals. It enables appropriate control over access to information assets and prevents identity theft using electronic certificates.

(1) Access Control via Authentication System
User identification and the granting of access authority by user are critical in providing access to information assets. So the NEC Group has built a centrally managed authentication platform, targeting not only our own employees, but business partners as well.

Authentication data includes a user ID, organizational data, title, and other access control information. Because this is linked to the human resources system and instantly reflects information on any job changes (between companies or divisions, changes in title, resignations, etc.), the system always maintains the latest information.

By linking to this authentication platform, NEC Group systems make it simple to configure settings for information access and other parameters based on organization or title.

The authentication platform has been rolled out to all domestic NEC Group companies using the NEC Intranet. For overseas subsidiaries, since 2008, the NEC Group has proceeded with the migration of platforms developed individually by each company to a common NEC Group authentication platform. In this manner, the NEC Group has centralized global management of information security measures, including prevention of information leak.

(2) Preventing Identity Theft through Electronic Certificates
When using particularly critical systems for ordering and other operations, authentication via electronic certificate is often used to lessen system risks caused by identity theft of users. Electronic certificate is a kind of electronic personal identification (a digital ID) and a stricter method than a simple user ID and password. It is stored on the IC chips embedded in employee ID badges.

In addition, by linking the NEC Group authentication platform with third-party certification authorities, we are able to issue electronic mail certificates providing NEC Group employees with authentication of themselves and their company. When sending important information such as customer information via email, these electronic mail certificates are used to securely exchange emails with S/MIME encoding. Email used as proof under internal controls or for Japan’s Financial Instruments and Exchange Law (J-SOX) compliance can also be signed electronically using these electronic mail certificates, providing comprehensive proof of the identity of the sender.

IT Platform for User Management and Control

Authentication systems are the foundation of information security management. The NEC Group built a system to identify individuals. It enables appropriate control over access to information assets and prevents identity theft using electronic certificates.

(1) Access Control via Authentication System
User identification and the granting of access authority by user are critical in providing access to information assets. So the NEC Group has built a centrally managed authentication platform, targeting not only our own employees, but business partners as well.

Authentication data includes a user ID, organizational data, title, and other access control information. Because this is linked to the human resources system and instantly reflects information on any job changes (between companies or divisions, changes in title, resignations, etc.), the system always maintains the latest information.

By linking to this authentication platform, NEC Group systems make it simple to configure settings for information access and other parameters based on organization or title.

The authentication platform has been rolled out to all domestic NEC Group companies using the NEC Intranet. For overseas subsidiaries, since 2008, the NEC Group has proceeded with the migration of platforms developed individually by each company to a common NEC Group authentication platform. In this manner, the NEC Group has centralized global management of information security measures, including prevention of information leak.

(2) Preventing Identity Theft through Electronic Certificates
When using particularly critical systems for ordering and other operations, authentication via electronic certificate is often used to lessen system risks caused by identity theft of users. Electronic certificate is a kind of electronic personal identification (a digital ID) and a stricter method than a simple user ID and password. It is stored on the IC chips embedded in employee ID badges.

In addition, by linking the NEC Group authentication platform with third-party certification authorities, we are able to issue electronic mail certificates providing NEC Group employees with authentication of themselves and their company. When sending important information such as customer information via email, these electronic mail certificates are used to securely exchange emails with S/MIME encoding. Email used as proof under internal controls or for Japan’s Financial Instruments and Exchange Law (J-SOX) compliance can also be signed electronically using these electronic mail certificates, providing comprehensive proof of the identity of the sender.
The IT platform for PC and network protection is designed to maintain the security of all information devices connected to the NEC Intranet and protect the network from viruses, worms, and other attacks. The system provides monitoring and controls to ensure secure use of the Intranet, including restricting access from PCs with security problems, and running periodic vulnerability scans.

(1) Protecting PCs from Cyber-Attacks
(Monitoring Security Patch Updates)
New vulnerabilities are being found in OSs and software every day. To protect them from attacks by malicious programs, it is necessary to strictly apply the security patches that address these vulnerabilities.

At the NEC Group, installation of software to monitor PC and network status is required for all PCs connecting to the NEC Intranet, enabling us to visualize the status. This makes it possible to monitor whether the necessary security patches for OS and software have been applied, send messages to the user if they have not been applied, and restrict network access after a while.

The system can also check any security patches installed on the PC, and display messages on the PC warning the user to install or update the software as needed.

(Implementation of Anti-Virus Measures)
We have standardized anti-virus software and security settings for all PCs to prevent the spread of virus and worm infections.

If the system finds an unsecure PC, the PC is quickly isolated from the Intranet.

---

**Figure: IT Platform for PC and Network Protection**

- **User Environment Support**
  - Strengthen Management
    - Monitor Information on Network-Connected Devices
    - Collection of information on network connection status
  - Monitor Information on PC
    - Hardware and software information, patch information, etc.
  - Distribute Policies
  - Distribute Updated Virus Definitions
  - Distribute Patches

- **Network Management**
  - Prompt Detection, Localization and Restoration
    - Network Surveillance
      - Automation of network disconnection/restoration
    - Intrusion Detection
      - Detection of improper packets
    - Router Management
      - Centralized management of router configuration

---

**Ensure Secure and Reliable Intranet Use**
To prevent information leak, it is necessary to identify the illegal route by which information is being distributed and to put in place appropriate measures based on a risk analysis. The NEC Group manages not only our own Group information but information from customers and information disclosed to suppliers. We maintain comprehensive measures based on the characteristics of networks, PCs, electronic media, and other IT components.

(2) Vulnerability Scans
Information devices running on a variety of platforms, such as Windows, UNIX, LINUX, and Mac, connect to the NEC Intranet.

We check the status of all information devices via our network by vulnerability scans.
Managers in each division are able to view the status and address any vulnerabilities using specified methods.
We can check the status of addressing the vulnerabilities across the NEC Group.
By scanning vulnerabilities on a regular basis, we make it possible to address new vulnerabilities and thus maintain security levels.

IT Platform for Information Protection

To prevent information leak, it is necessary to identify the illegal route by which information is being distributed and to put in place appropriate measures based on a risk analysis. The NEC Group manages not only our own Group information but information from customers and information disclosed to suppliers. We maintain comprehensive measures based on the characteristics of networks, PCs, electronic media, and other IT components.

(1) System to Prevent Information Leak
The NEC Group has built a system to prevent information leak using its proprietary InfoCage system. Specifically, the system encrypts hard disks and files, restricts use of USB flash drives and other external storage media, and monitors PC operations. The system has proved to be enormously effective in preventing information leak.
(Hard Disk Encryption)
All business PCs in the NEC Group have InfoCage PC security software installed. This ensures that all data on the PC are stored in an encrypted state. This prevents the leak of critical information in case of theft or loss, thereby minimizing damages.

(Restrictions on Use of External Storage Media)
In the NEC Group, USB flash drives and other external storage media used in business must be standardized models with a forced encryption feature. To prevent information from being removed, stolen, or lost through use of personal, off-the-shelf media, PCs are also configured to write data only to standardized media. Specific policies regarding such controls are applied on a mandatory basis using the Policy Receipt Client installed on each PC. This makes it possible to use external storage media approved by the relevant manager in each company or division.

(Logging of PC Operations)
When incidents of information leak occur, it is necessary to accurately understand circumstances surrounding the incident, minimize the impact of the leak, and enact measures to prevent a recurrence. By storing PC operation logs, it is possible to investigate the impact of the leak and analyze the incident with accuracy.

(Automatic File Encryption)
We have implemented a file access control system, which automatically encrypts files exchanged within the Group and restricts access to those files only to authorized users. This system enables them to access and edit encrypted files and, because encrypted files can only be decrypted by limited users, information cannot be leaked even if the file falls into the hands of a third party. This enables a higher level of security than with traditional file encryption methods. We have extended these information leak prevention measures across our entire value chain, by making file access controls available to our suppliers as well.

(2) System to Prevent Misdelivery of Emails
Information leak incidents can arise from mistakes—an incorrectly entered email address, or a file attached in error. So, we have implemented a system to prevent misdelivery of emails. It ensures that the addressee and attachment information for all email sent outside the company is checked prior to sending. It is also possible to set restrictions so that, for example, the mail cannot be sent until a supervisor or other third party checks the addressee, content, etc. This leads to an even further reduction in errors and prevents information leak due to deliberate forwarding of email, etc.

(3) Secure Information Exchange Site
The NEC Group operates a Secure Information Exchange Site, which makes possible the safe, secure exchange of important information with customers and suppliers. The system uses a one-time URL (an address that can only be connected to once) and password system to provide a secure exchange of files. This eliminates the need to carry USB flash drives and other external storage devices, and reduces the risk of information leak incidents through the theft or loss of such devices.
(4) Thin Clients
To prevent information leak, streamline operations, and reduce the total cost of ownership (TCO), in fiscal 2007 the NEC Group introduced the Thin Client Service. Since starting with only 100 PCs, the system had expanded to cover 13,000 PCs by fiscal 2010. It is now the largest virtual PC-type thin client system in Japan.

For the thin client server, NEC chose to employ an easy to manage and environmentally friendly virtual PC system, which requires only a handful of system engineers for all of the virtual PCs. During server maintenance, for example, this system makes it possible to transfer the virtual PC environment to another server without interrupting operations. The thin client terminals being provided include desktop models (US110 and US300a), lightweight mobile devices (US10Na), as well as installation kits to convert existing PCs to thin client terminals.

With the spread of this Thin Client Service, and as a measure against theft or loss of laptop PCs, rules for removing PCs from the workplace were strengthened in fiscal 2009. The rules require all employees to use thin client terminals for work outside of the office. This has resulted in a significant reduction in incidences of information leak.

Beginning in July 2008, the NEC Group also started a home-based work system. The system uses thin client terminals to minimize the risk of information leak that can occur at home. In November 2009, we prepared a simplified software-based thin client as part of our measures against the new influenza strain, ensuring that operations related to social infrastructure could be maintained even in the event of a pandemic.
The NEC Group develops human resources with expert knowledge and skills relating to information security to meet the expectations of customers, business partners, the general public and the market.

Framework of Information Security Human Resources Development

The NEC Group focuses on three categories of human resources development for information security: 1) knowledge and awareness 2) promotion of security measures and 3) a certification system for information security professionals.

Improving Knowledge and Increasing Awareness of Information Security

To maintain and improve information security, it is important for each and every employee to act appropriately in accordance with the NEC Group information security policies. The NEC Group runs a variety of training programs to ensure that employees have a thorough understanding of information security policy and personal protection policy, and that they act properly in accordance with those policies.

(1) Training on Information Security and Personal Information Protection

All employees use a web-based training system called Learning Door, NEC’s human resources development platform, to acquire essential knowledge on the subject of information security and to increase awareness. We review the contents of the information security training and updates them every year so that the training curriculum incorporates specific information on security incidents and practical issues in real business scenes. At overseas subsidiaries, more employees will take part in the course in fiscal 2011 to reinforce information security on a global level.

(2) Enforcement of “Basic Rules for Customers Support”

With the objective of ensuring the security of customer information and personal information, we compiled “Basic Rules for Customers Support,” which state the minimum rules that must be followed. Electronic Pledge System is used by the NEC Group employees and our suppliers to confirm that they agree to observe the rules.

(3) Workplace Meetings on Information Security

The NEC Group conducts meetings on information security at each workplace using case studies. The purpose of these meetings is to share security information and raise security awareness through active dialog and to help with the resolution of security issues at the workplace. Effective activities have been held at many workplaces. The activities included Video-based training on the importance of information security, training on risk prediction, and discussions on various topics (for example management of confidential information, how to prevent email address errors, and conduct risk analysis).
The NEC Group has assigned and trained information security promoters who play an important role in implementing security measures.

(1) Development of ISM Leaders
Information security management (ISM) leader training provides promoters at each division level with the necessary practical knowledge and skills to encourage information security measure. Instructors with extensive practical experience teach promotion strategies through video-based training and case studies. The training also provides the promoters in training with a good opportunity to share information on their experiences and issues regarding security measures in each division.

(2) Development of Information Security Assessors
The NEC Group has established the Information Security Standards for suppliers. The standards enable us to raise the efficiency of information security assessment of suppliers. And we also train the assessors and accumulate practical know-how on information security. Training sessions on this subject were held seven times in fiscal 2010, and approximately 90 employees completed the session. We intend to improve the level of information security at NEC Group suppliers by information security assessors.

The NEC Group has developed information security professionals to provide value-added products, services and solutions in this area for our customers.

(1) NEC Certified Professional System
We have built “NEC Certified Professional” System. Employees with advanced skills and public certifications related to information security are certified as technical specialists in the area of security in the NEC Group. Security skills are required to the specialists in other areas, for example, IT service management and network construction. Certified specialists play a key role in ensuring the security of products, services and solutions for customers.

(2) NEC Skill Certification Program
NEC Skill Certification Program uses computer-based testing (CBT) to certify technical competence and practical skills of products and services provided by NEC and independent software vendors (ISV). The purposes of this program are to: 1) enhance customer trust by improving the skill levels of employees 2) disclose skills to promote business 3) prompt employee career development. The CBT examination in NEC Skill Certification Program covers some subjects focusing on information security.
To protect customer information, the NEC Group conducts information security measures with the suppliers on our supply chain, and continues to expand the number of participating companies.

Framework

NEC Group business activities are conducted in partnership with suppliers. We recognize that it is extremely important for suppliers not only to have technical ability but also to maintain information security.

The information security measures that we require of our suppliers are classified into the following six major categories.

1. **Contract Management**
   - General prohibition on subcontracting, confidentiality obligation, personal information protection, etc.

2. **Subcontracting Management**
   - Prior approval required when subcontracting unavoidable

3. **Staff Management**
   - Implementation of Basic Rules for Customers Support

4. **Confidential Information Management**
   - Implementation of Confidential Information Management Guidelines

5. **IT-based Measures**
   - Required measures and recommended measures

6. **Assessment**
   - On-site assessment of implementation of Information Security Standards for Suppliers and web-based self assessment

Overview of the Measures

**(1) Contract Management**

All contracts between the NEC Group and suppliers are comprehensive agreements that include clauses prohibiting subcontracting in principle, maintaining confidentiality and protecting personal information. In addition, memorandums of understanding (MOUs) are concluded concerning the management of workers that handle information belonging to the NEC Group or our customers. These MOUs mainly require that workers handling such information pledge to their own companies that they understand the security measures and will fully comply with them.

**(2) Subcontracting Management**

Subcontracting by suppliers to other companies is forbidden in principle. If subcontracting cannot be avoided, information on the subcontractor must be submitted to the original contractor in the NEC Group and prior approval must be granted by the original contractor.

**(3) Worker Management**

The NEC Group established “Basic Rules for Customers Support”, which are security measures requested for suppliers. We promote compliance with these rules through the use of the aforementioned MOUs.

The rules reflect lessons which we learned from security incidents that have occurred in the same industry. They represent the collection of required individual practices and prohibited acts, which are described specifically and clearly.

**(4) Confidential Information Management**

Management of confidential information handled under NEC Group contracts is covered by Confidential Information Management Guidelines. We require compliance with these guidelines for each commissioned task and promote the implementation of management according to the guidelines.

The guidelines contain the following six sections:
(1) NEC Information Security Initiatives Seminars

NEC Information Security Initiatives Seminars are held from Hokkaido to Kyushu once or twice a year for approximately 2,000 suppliers nationwide. The seminars are run in collaboration between the Purchasing Division and the Information Security Division to ensure that suppliers understand and implement the NEC Group’s security measures.

(2) Training Sessions to Develop Instructors

Suppliers are requested to appoint in-house instructors to teach the aforementioned Basic Rules for Customers Support. We hold training sessions for instructors every year and give them certification (effective for one year). In fiscal 2010, approximately 1,200 instructors obtained or renewed certification.

(3) Distribution of Video on Confidential Information Management

In fiscal 2010, we distributed to suppliers a video on managing confidential information to raise awareness of the necessity and importance of confidential information management, and to promote the implementation of the Confidential Information Management Guidelines.

In fiscal 2011, we will distribute to suppliers an internal training support CD-ROM aimed at improvement of more practical skills on confidential information management.
To provide customers with “Better Products, Better Services” from a security perspective, the NEC Group conducts a variety of initiatives to ensure a high level of security for its products and services.

Incorporating Security into Development Processes

With the rapid development of the information society in recent years, ensuring the security of important information assets like personal information and trade secrets has become a matter of great concern.

To comply with industry standards and prevent incidents associated with the use of our products and services, the NEC Group is working to ensure a high level of security by building development processes that incorporate security considerations from the first stages of development (requirement definitions and design). We are doing so by constructing a company-level promotion framework, conducting training, providing various guidelines, improving divisional development standards, and facilitating rigorous implementation of related measures throughout the NEC Group.

As an example of an initiative to strengthen development standards, we defined specific procedures methodologically with SystemDirector Enterprise, the NEC Group’s system development standard, to improve security during system design and development. Developers apply the procedures to efficiently fulfill system security requirements.

<table>
<thead>
<tr>
<th>SECURITY-AWARE DEVELOPMENT PROCESSES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Divisional Development Standards</td>
</tr>
<tr>
<td>Requirement Definition</td>
</tr>
<tr>
<td>Life-cycle Management</td>
</tr>
<tr>
<td>Incorporating Security Tasks into Divisional Development Standards, etc.</td>
</tr>
<tr>
<td>Utilizing them as Quality Inspection Criteria (Phase migration, delivery decision, inspection conditions for outsourced work)</td>
</tr>
</tbody>
</table>

Security Tasks

- Recognition of Security Needs
- Threat Identification
- Determining Countermeasure Policy
- Forming Consensus
- Secure Interface Design
- Security Function Design
- Security Architecture Design

Requirement Definition Phase

- Check

Design Phase

- Check

Security Technology Guidelines

- Comply with Industry Standards, International Standards (ISO/IEC 15408), etc.
Addressing Vulnerabilities

When development takes place while incorporating security considerations it becomes possible to eliminate many vulnerabilities, which are security defects. However, new vulnerabilities are detected every day, even in operating systems and libraries already in use. And it is not possible to address vulnerabilities that are not yet known. If a system administrator does not quickly address known vulnerabilities, information leaks, unauthorized operations or virus infections could occur.

The NEC Group is therefore focusing on management of vulnerability information. We have developed a vulnerability information management system that draws on our accumulated know-how in this area. The system promptly conveys detailed information on causes and measures of vulnerability to the relevant developers when a vulnerability is discovered, for example, in a product that has already been delivered. The system also manages measures by each project and gives a warning if the measure has not been implemented. This ensures that appropriate measures are applied. For customers, we are building a system that will link to this management system and promptly disclose vulnerabilities information on NEC products.

Providing Reliable Security through Third-Party Certification

We strive to guarantee that security requirements are properly met and ensure that our products and services can be used by customers with complete peace of mind. So the NEC Group is working to improve security by promoting the attainment of ISO/IEC 15408 certification (the international IT security standard) for our software products, which include WebSAM, InfoCage, WebOTX and StarOffice. Group companies have assigned dedicated promoters for this initiative and created a framework for quickly obtaining certification. Certification is also being obtained for System to Prevent Information Leak used internally and Secure Information Exchange Site used with customers so that customer information is appropriately protected and customers can transact with the NEC Group with total confidence.

Obtaining ISO/IEC 15408 CERTIFICATION FOR WebOTX SERVICE EXECUTION INFRASTRUCTURE

Developers design and implement security functions for potential threats on application servers (unauthorized log-ons, unauthorized use, operation errors, abnormal shutdowns, etc.). Evaluators inspect from a third-party perspective based on the international ISO/IEC 15408 standard and guarantee that security functions have been designed and implemented appropriately.
Cloud computing, a major trend in how information technology is utilized, will make information security even more important in the years ahead. The NEC Group will leverage our practical, proprietary know-how to provide security solutions that are trusted by our customers.

NEC’s Approach to Security Solutions

The NEC Group has an extensive lineup of security solutions that we provide in optimal combinations to customers to solve the security issues they face. We have provided solutions to reduce IT costs and eliminate process inefficiencies by visualizing the IT environment and by automating management.

With the recent changes in the economy, efficient IT investment is now needed. Cloud computing has attracted attention in recent years as a solution for IT investment. However, customers face the new challenge of strengthening internal security against more complex and sophisticated threats, selecting effective cloud services, and securely and smoothly integrating internal networks with cloud services.

The NEC Group has systematized the know-how we have acquired in building and operating internal systems with 140,000 users to provide security solutions for overcoming these new challenges. The solutions cover information security measures in IT and network domains. We provide the solutions to various issues from system requirement definitions to development and construction for customers.
We aim to speed up management, visualize consolidated performance, strengthen internal controls and substantially reduce TCO. So the NEC Group is currently implementing integrated management reforms on business structure reforms, business process reforms and IT system reforms. As we do so, we are consolidating core IT systems, built and operated independently by various Group companies, into a cloud environment to be utilized as a shared Group management platform.

Each NEC division and NEC Group company will promote “IT, without owning it” by utilizing the functions they need that are provided by the shared platform as a service rather than owning all the IT systems internally.

Servers, storage media and other resources for the cloud environment are housed at multiple large-scale datacenters where security is assured. The datacenters are protected by strict physical security, including monitoring with infrared sensors and surveillance cameras and access control with fingerprint and IC card authentication. Datacenters are located at multiple sites separated by several hundred kilometers. So there is very little possibility of the system being shut down by a natural disaster that simultaneously affects all the sites. In addition, we use platform products based on our next-generation IT platform called REAL IT PLATFORM G2. Moreover, the datacenters strictly manage user authorization based on different job duties, conduct change and release management automated on the system, monitor logs on a regular basis. This keeps system operating stable and ensures robust security.

We established an NEC Cloud Plaza showroom on the first floor of the NEC headquarters building in October 2009 to provide visitors with the opportunity to directly experience cloud-oriented service platform solutions. Drawing on the know-how acquired in developing our own management system, these solutions constitute a complete package from business process reform to system provision and operation.

Utilizing cloud computing carries the benefit of greater process efficiency and lower costs. Nevertheless, many customers are concerned about turning over their information to an outside party, about service stability, and about integration with internal systems. That is why the NEC Group systematizes security measures proven on our own systems. We provide customers with security solutions that enhance public safety and security for cloud computing.

For example, we provide a solution for integrating user management within a company and enabling single sign-on for internal systems and cloud services as well as a solution for preventing information from leaking to unauthorized parties by managing access in a company for information placed in the cloud environment. Our robust support allows customers to use the cloud environment with complete confidence.
The NEC Group proactively obtains third-party evaluations and certifications related to information security.

## ISMS Certification

The following companies have units that have obtained ISMS (ISO/IEC 27001) certification, an international standard for information security management systems.

<table>
<thead>
<tr>
<th>NEC Group Companies with ISMS Certified Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEC Corporation (29 business units and organizations)</td>
</tr>
<tr>
<td>NEC AccessTechnica, Ltd.</td>
</tr>
<tr>
<td>ABeam Consulting Ltd.</td>
</tr>
<tr>
<td>ABeam Systems Ltd.</td>
</tr>
<tr>
<td>N&amp;J Financial Solutions Inc.</td>
</tr>
<tr>
<td>NEC Engineering, Ltd.</td>
</tr>
<tr>
<td>auraline Corporation</td>
</tr>
<tr>
<td>NEC Capital Solutions Limited</td>
</tr>
<tr>
<td>NEC Software Kyushu, Ltd.</td>
</tr>
<tr>
<td>KIS Co., Ltd.</td>
</tr>
<tr>
<td>NEC Aerospace Systems, Ltd.</td>
</tr>
<tr>
<td>NEC Computertechno, Ltd.</td>
</tr>
<tr>
<td>NEC Saitama, Ltd.</td>
</tr>
<tr>
<td>NEC Shizuokabusiness, Ltd.</td>
</tr>
<tr>
<td>NEC System Technologies, Ltd.</td>
</tr>
<tr>
<td>NEC Informatec Systems, Ltd.</td>
</tr>
<tr>
<td>Showa Optronics Co., Ltd.</td>
</tr>
<tr>
<td>NEC Soft, Ltd.</td>
</tr>
<tr>
<td>NEC Software Tohoku, Ltd.</td>
</tr>
<tr>
<td>NEC Soft Okinawa, Ltd.</td>
</tr>
<tr>
<td>NEC Software Chubu, Ltd.</td>
</tr>
<tr>
<td>NEC Communication Systems, Ltd.</td>
</tr>
<tr>
<td>NEC Design &amp; Promotion, Ltd.</td>
</tr>
</tbody>
</table>

(As of March 31, 2010)
Privacy Mark Certification

The following companies have been licensed by the Japan Information Processing Development Corporation (JIPDEC) to use the Privacy Mark.

<table>
<thead>
<tr>
<th>NEC Group Companies with Privacy Mark</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEC Corporation</td>
</tr>
<tr>
<td>NEC AccessTechnica, Ltd.</td>
</tr>
<tr>
<td>NEC Infrontia Corporation</td>
</tr>
<tr>
<td>N&amp;J Financial Solutions Inc.</td>
</tr>
<tr>
<td>NEC Engineering, Ltd.</td>
</tr>
<tr>
<td>NEC Software Kyushu, Ltd.</td>
</tr>
<tr>
<td>KIS Co., Ltd.</td>
</tr>
<tr>
<td>NEC Control Systems, Ltd.</td>
</tr>
<tr>
<td>NEC Computertecho, Ltd.</td>
</tr>
<tr>
<td>CyberWing Corporation</td>
</tr>
<tr>
<td>NEC Shizuokabusiness, Ltd.</td>
</tr>
<tr>
<td>NEC System Technologies, Ltd.</td>
</tr>
<tr>
<td>NEC Informtec Systems, Ltd.</td>
</tr>
<tr>
<td>NEC Soft, Ltd.</td>
</tr>
<tr>
<td>NEC Software Tohoku, Ltd.</td>
</tr>
<tr>
<td>NEC Soft Okinawa, Ltd.</td>
</tr>
<tr>
<td>Chugoku Sunnet Corporation</td>
</tr>
<tr>
<td>NEC Software Chubu, Ltd.</td>
</tr>
<tr>
<td>NEC Display Solutions, Ltd.</td>
</tr>
<tr>
<td>NEC Design &amp; Promotion, Ltd.</td>
</tr>
<tr>
<td>SGI Japan, Ltd.</td>
</tr>
<tr>
<td>NEC Nexsolutions, Ltd.</td>
</tr>
<tr>
<td>NEC Networks &amp; System Integration Co., Ltd.</td>
</tr>
<tr>
<td>NEC Net Innovation, Ltd.</td>
</tr>
<tr>
<td>NEC Personal Products, Ltd.</td>
</tr>
<tr>
<td>VALWAY121Net, Ltd.</td>
</tr>
<tr>
<td>NEC Business Processing, Ltd.</td>
</tr>
<tr>
<td>NEC BIGLOBE, Ltd.</td>
</tr>
<tr>
<td>NEC Facilities, Ltd.</td>
</tr>
<tr>
<td>NEC Fielding, Ltd.</td>
</tr>
<tr>
<td>Forward Integration System Service Co., Ltd.</td>
</tr>
<tr>
<td>NEC Professional Support, Ltd.</td>
</tr>
<tr>
<td>NEC Software Hokuriku, Ltd.</td>
</tr>
<tr>
<td>NEC Software Hokkaido, Ltd.</td>
</tr>
<tr>
<td>NEC Magnus Communications, Ltd.</td>
</tr>
<tr>
<td>NEC Mobility, Ltd.</td>
</tr>
<tr>
<td>NEC Livex, Ltd.</td>
</tr>
<tr>
<td>NEC Learning, Ltd.</td>
</tr>
<tr>
<td>LIVANCE-NET Ltd.</td>
</tr>
<tr>
<td>NEC Logistics, Ltd.</td>
</tr>
<tr>
<td>Yokohama Electronic Computing &amp; Solutions Co., Ltd.</td>
</tr>
</tbody>
</table>

(As of March 31, 2010)

IT Security Evaluation and Certification

The following lists major products and systems that have obtained ISO/IEC 15408 certification, an international standard for IT security evaluations.

<table>
<thead>
<tr>
<th>NEC Products and Systems with ISO/IEC 15408 Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>· StarOffice X (Groupware product)</td>
</tr>
<tr>
<td>· WebSAM SystemManager (Server management software product)</td>
</tr>
<tr>
<td>· InfoCage PC Security (Preventing information leak software product)</td>
</tr>
<tr>
<td>· WebOTX Application Server (Application server software product)</td>
</tr>
<tr>
<td>· NEC Group Secure Information Exchange Site</td>
</tr>
<tr>
<td>· NEC Group System to Prevent Information Leak</td>
</tr>
<tr>
<td>· NEC Firewall SG Core Unit (Firewall software product)</td>
</tr>
<tr>
<td>· PROCENTER (Document management software product)</td>
</tr>
</tbody>
</table>

(As of March 31, 2010)
Corporate Data

Company name: NEC Corporation
Address: 7-1, Shiba 5-chome, Minato-ku, Tokyo, Japan
Established: July 17, 1899
Capital: ¥397.2 billion
Number of employees (Consolidated): 142,358
Consolidated Subsidiaries: 310

IT Services Business
NEC supplies government agencies and private-sector companies with a range of IT services covering systems implementation, maintenance and support, and outsourcing.

Platform Business
NEC supplies customers with products composing corporate internal networks, including IP telephone systems and wireless LANs, in addition to products essential to the implementation of IT systems, including servers, supercomputers, storage equipment and software.

Carrier Network Business
NEC supplies equipment required in network implementation to communications service providers, along with network control platform systems and operating services.

Social Infrastructure Business
NEC supplies industrial systems that support social infrastructure, including broadcasting systems, artificial satellites and integrated CCTV surveillance systems for airports and local governments, as well as other security-related systems that enhance public safety and security.

Personal Solutions Business
NEC provides mobile handsets, personal computers and other terminals to the ubiquitous networking society, as well as “BIGLOBE” Internet services. NEC is also developing new services that combine all of those elements.
“The NEC Way” is the collective activities of NEC Group management. This consists of our Corporate Philosophy, Vision, Core Values, Charter of Corporate Behavior, and Code of Conduct. We put The NEC Way into practice to contribute to our customers and society so as to create an information society that is friendly to humans and the earth.

[NEC Group Corporate Philosophy]

NEC strives through “C&C”
to help advance societies worldwide
toward deepened mutual understanding
and the fulfillment of human potential.

Established in 1990

[NEC Group Vision 2017]
The NEC Group Vision 2017 states what we envision as a company, and the society which we will strive to realize in 10 years, in pursuing our Corporate Philosophy. We set our Group Vision “2017,” since that year will mark exactly 40 years since “C&C,” the integration of Computers and Communications, was presented.

To be a leading global company
leverage the power of innovation
to realize an information society
friendly to humans and the earth
[NEC Group Core Values]
To pursue our Corporate Philosophy and realize NEC Group Vision 2017, we have defined the values important to the NEC Group, which is built on over 100 years' history of our company. This is what we base our behaviors and individual activities on, as a guidance to better serve our customers and contribute to society.

<table>
<thead>
<tr>
<th>Core Values</th>
<th>Actions driven by Core Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Our motivation]</td>
<td>maze_1</td>
</tr>
<tr>
<td>Passion for Innovation</td>
<td>■ Explore and grasp the real essence of issues ■ Question the existing ways and develop new ways ■ Unite the intelligence and expertise around the world</td>
</tr>
<tr>
<td>[As an individual]</td>
<td>maze_2</td>
</tr>
<tr>
<td>Self-help</td>
<td>■ Act with speed ■ Work with integrity until completion ■ Challenge beyond own boundary</td>
</tr>
<tr>
<td>[As a team member]</td>
<td>maze_3</td>
</tr>
<tr>
<td>Collaboration</td>
<td>■ Respect each individual ■ Listen and learn with open mind ■ Collaborate beyond organizational boundaries</td>
</tr>
<tr>
<td>[For our customers]</td>
<td>maze_4</td>
</tr>
<tr>
<td>Better Products, Better Services</td>
<td>■ Think from a user’s point of view ■ Impress and inspire our customers ■ Continue the pursuit of “Global Best”</td>
</tr>
</tbody>
</table>

[NEC Group Charter of Corporate Behavior]
The NEC Group works to improve profitability through sound business activities and to achieve dynamic development so as to benefit society. To this end, the Group is aware of the need to enhance its corporate value not only by observing all relevant laws and regulations, but also by fulfilling its social responsibilities as a good corporate citizen. At the same time, the Group must win the trust of customers, shareholders, investors, suppliers, the community at large, its employees, and all other stakeholders.

Attaining Customer Satisfaction
The NEC Group earns customer satisfaction and confidence by developing and offering beneficial and reliable products and services and by paying careful attention to safety.

Developing New Technologies
The NEC Group strives to develop creative technologies and works actively to break ground in new business areas for the future prosperity of society.

Conducting Fair Corporate Activities
The NEC Group promotes fair, transparent, and free competition between corporations and ensures that its relationships and dealings with government agencies and political bodies are of a normal and proper nature.

Disclosing Information
The NEC Group delivers accurate and sufficient corporate information in a timely, clear, and appropriate manner while enhancing the transparency of its corporate activities.

Preserving the Global Environment
The NEC Group reduces the impact on the global environment and contributes to building a sustainable society.

Maintaining Good Relations With the Community
The NEC Group respects the customs and cultures of all regions and countries and manages its activities in a way that contributes to community development.

Conducting Thoughtful Corporate Citizenship Activities
The NEC Group fully recognizes that it is a key member of society and actively engages in philanthropy and other activities of social benefit as a good corporate citizen.

Protecting Human Rights
The NEC Group respects human rights in all its corporate activities, never accepting any discriminatory practices or child or forced labor.

Valuing Employees
The NEC Group respects each employee’s individuality and creates work environments where all its employees can fully demonstrate their abilities and carry out their jobs with enthusiasm.

Protecting Intellectual Property and Personal Information
The NEC Group recognizes the value of intellectual property and personal information and properly manages them.
To contribute to society by offering better products and services, we consider it to be our duty to protect the information assets we keep for our customers and partners as well as our own information assets. To achieve this, NEC Corporation (“NEC”) declares the adoption of this information security statement and its implementation.

- NEC makes efforts to maintain an information security management system and to control its information assets appropriately.
- NEC builds up its internal rules and regulations so that they are in line with this statement.
- NEC continuously offers the training that is necessary to maintain information security.
- NEC implements human, organizational, and technological security controls to protect its information assets from unauthorized access, leakage, modification, theft/loss, denial of service attacks, or any other threat.
- NEC makes efforts to rapidly locate the root cause, keep damage to a minimum and prevent the recurrence if an incident posing a threat to information assets should occur.
- NEC complies with the laws and regulations as well as the national guidelines, the social standards and norms related to information security.
- NEC continuously reviews and improves those activities listed above.

By offering various Internet-related products, services, and solutions, NEC Corporation (“NEC”) contributes to society as a global leading company which realizes an “information society friendly to humans and the earth” through innovation.

In working toward the realization of such a society, NEC recognizes that the protection of personal information is its social responsibility and has established a policy for the protection of personal information. Efforts are constantly being made to implement and maintain the policy. This privacy policy sets forth our principles as follows (note that the original is in Japanese):

- NEC obtains, uses and provides personal information properly based on Japanese Industrial Standard’s “Personal Information Protection Management Systems - Requirements (JIS Q 15001:2006).” NEC assigns a person in charge of protecting personal information at each of its relevant divisions, taking account of its organizational structure. Among other things, NEC takes appropriate measures not to handle personal information other than for the specified purposes.
- NEC abides by the laws, regulations and guidelines of Japan pertaining to the protection of personal information.
- NEC makes efforts to implement, through the adoption of necessary and appropriate security measures, the security control of personal information handled by NEC, including protection from disclosure, loss or damage.
- NEC appropriately responds to complaints and requests for consultation with respect to NEC’s handling of personal information and its personal information protection management system. Please contact the designated person or place for inquiries.
- NEC makes efforts to continuously improve its personal information protection management system, including this policy.