NTT DATA
Global IT Innovator

Information Security Report 2012

NTT DATA Corporation

Corporate Philosophy

(Mission of the NTT DATA Group)

NTT DATA Group utilizes information technology to create new paradigms and values, contributing to the achievement of a more affluent and harmonious society.

Applicable period and timing of this report

- This report applies to all information covered by the NTT DATA Group.
- This report applies to information security initiatives current at the end of December 2011 unless otherwise noted.

Scope of this report

NTT DATA Group (223 companies, including NTT DATA Corporation)
* Current as of December 31, 2011

Department in charge

NTT DATA Corporation
Information Security Office, Quality Assurance Department

Inquiries

NTT DATA Corporation
Information Security Office,
Quality Assurance Department
Toyosu Center Building
3-3-3, Koto-ku, Tokyo 135-6033
TEL: 050-5546-2545
URL: http://www.nttdata.co.jp/

CONTENTS

For an affluent, sustainable society

IT and information security for an ever-evolving society

2011 was a year of great change.
The Great East Japan Earthquake that struck in March required Business Continuity Plans (BCP) to be put in place, while subsequent restrictions to power consumption called for greater power-saving measures. There were also reports from other companies of hacker groups breaking through defenses and leaking large amounts of customer information, or information leaks following major government agencies or vital corporations being targeted as part cyber attacks. 2011 was indeed a year that called for reviews of information security policies.
We have also seen devices such as smartphones and tablets, and cloud services increasing in popularity and becoming more prominent in the business world. Companies have placed a priority on distributing information via social networking services (SNS) such as Twitter and Facebook.
It is not just the IT service industry that is changing – the entire globe is undergoing massive environmental change and experiencing advances in technology. Each and every company needs to implement a range of policies to combat these changes.

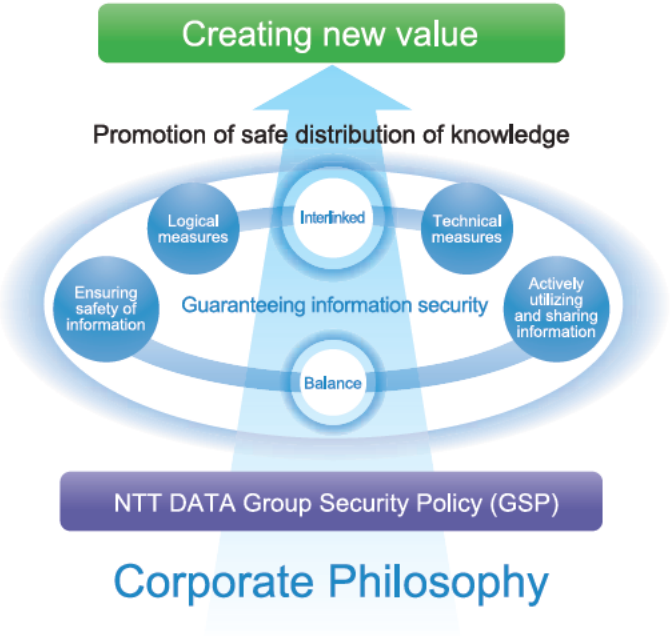
The NTT DATA Group covers countless large-scale systems required for running social infrastructure, and mission-critical systems essential for customer business strategies. The entire group is fully aware that customers place a great deal of faith in these systems. To ensure that customers are able to maintain complete trust in the NTT DATA Group, a range of initiatives have been implemented to prevent incidents related to information security from occurring at all.
The NTT DATA Group has developed a common "Group Security Policy" that applies to the entire group. With both a technical and logical approach, this policy aims to safely protect information as well as utilize information to create the optimum state for information security. The first information security report as a system integrator was created and released in 2008.
Now in its third edition, this report outlines the specific measures for implementing information security activities taken by the group to meet the ever evolving demands of an information-based society. I would be delighted if stakeholders reading through this report find it useful in one way or another.

NTT DATA Corporation
Representative Director and Senior Executive Vice President CISO

Toshio Iwamoto

NTT DATA Group information security policies

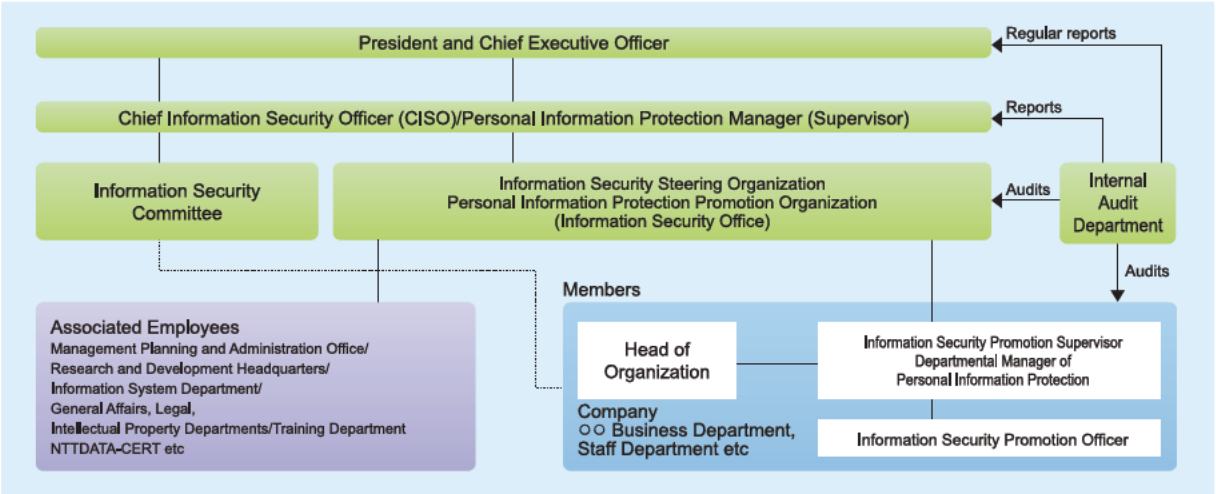
By maintaining an appropriate balance between ensuring safety of information and actively utilizing and sharing information, the NTT DATA Group applies its knowledge throughout the entire group and provide brand new value to customers.
Both logical measures covering the development of rules and providing training and educational activities related to information security, and technical measures for preventing leakages of information or the installation of thin-client PCs are required for adequately ensuring safety of information and actively utilizing and sharing information.



Development of "Information Security Policy" and "Personal Information Protection Policy"

NTT DATA is fully aware that leakage or unauthorized use of information due to security breaches can lead to major problems, and has focused on initiatives related to information security management from an early stage. More specifically, the "Information Security Policy" was developed in December 1998 with the aim of handling information assets appropriately, and ensuring the utmost information security.
The protection of personal information has long been identified as a factor requiring the highest level of priority, and has been assigned as a core activity of corporate management. In addition to establishing the "Personal Information Protection Policy" in July 2001, internal compliance regulations have been set to ensure that personal information is handled appropriately. The Personal Information Protection Policy and internal compliance regulations are reviewed and improved regularly to meet constant advances being made to information technology and changes in social conditions.

■NTT DATA Information Security, Personal Information Protection Activity Systems



Information security throughout the entire group

Standardizing key management policies and rules is essential, even at overseas offices, to ensure group and global management. The same concept applies to information security.
The NTT DATA Group developed standardized information security rules called "NTT DATA Group Security Policy (GSP)" in April 2008. Each company within the group has defined its own information security policy based on this GSP to suit the size and type of business of each particular company.
GSP also defines rules on how to handle information. This has allowed the entire NTT DATA Group to handle information safely.
Various systems have been designed and organized, including a group-wide network (GWNet), file transfer system (ETRANPOT), and document management system (Docφ), as part of an information distribution infrastructure for distributing electronic information throughout the group safely and efficiently.
A technical information knowledge bank (Solution Warehouse®, TeSS) designed to share knowledge between all group employees, encourages information to be utilized and shared safely, and serves to increase the competitive prowess of the entire group.

Example of Information Distribution Infrastructure

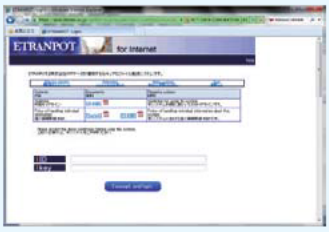
GWNet — All information sharing services are rolled out via GWNet on network infrastructure used to connect NTT DATA Group companies.

Group EGG

The NTT DATA Group intranet portal site.
Includes information such as notifications and news releases for group employees.

ETRANPOT

System for transferring files securely between the NTT DATA, NTT DATA Group companies and customers.
Files cannot be stored for longer than a set period of time.



Docφ

The file-sharing system for use between NTT DATA, NTT DATA Group and contracted companies. Also allows access rights and version management.

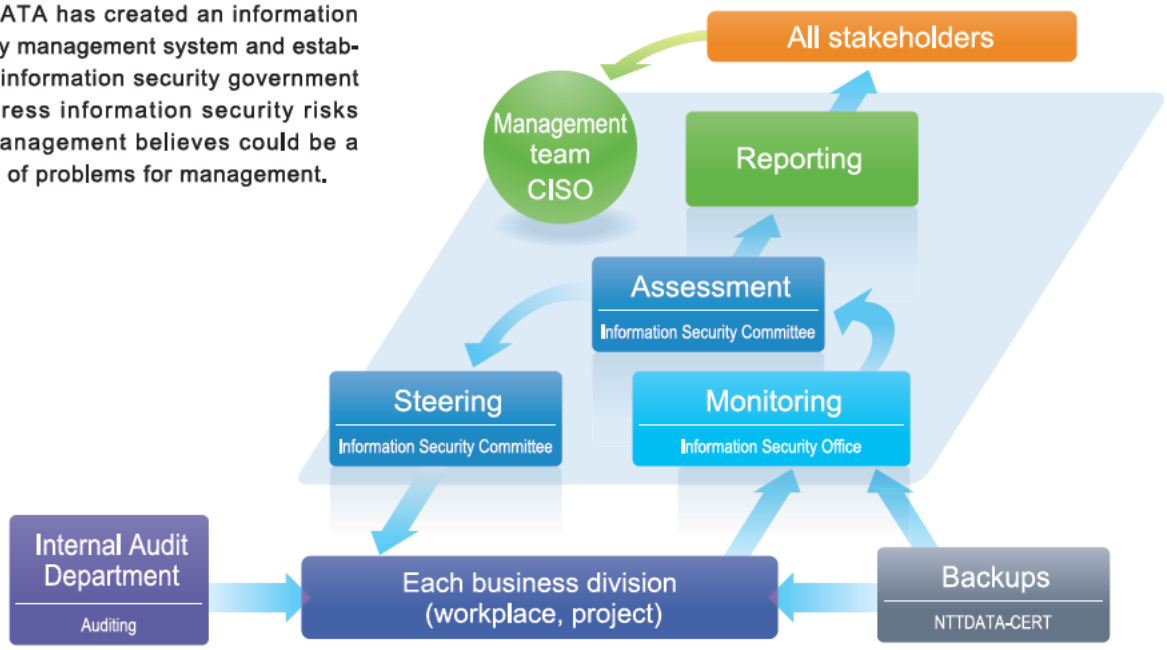
Solution Warehouse® / TeSS

Solution Warehouse®: NTT DATA Group technical information database.
TeSS: contact point for technical inquiries, and associated database.
Know-how is shared and utilized between the group.

NTT DATA information security management system

Establishing information security governance

NTT DATA has created an information security management system and established information security government to address information security risks that management believes could be a source of problems for management.



Steering — Information Security Committee

The Information Security Committee is overseen by the Representative Directors and Senior Executive Vice Presidents and CISO (Chief Information Security Officer), and held regularly with the managers of each department as members (held a total of 54 times to December 2011).

The Information Security Committee develops information security strategies for the NTT DATA Group with the aim minimizing information security risks, and ensuring safe utilization and sharing of information.

Monitoring — Information Security Office

Established as the special group for implementing information security activities throughout the NTT DATA Group.
This group conducts individual information security activities based on information security strategies, as well as monitoring of the implementation state of each information security activity.

Assessment

Information Security Committee

Information security implementation activities for this fiscal year are based on information security strategies, and are assessed as a whole with monitoring information of each activity, the results of internal audits and other factors. Each activity is reviewed based on the results of the assessment, and proposals are made for new information security strategies.

Auditing

Internal Audit Department

The Internal Audit Department at NTT DATA conducts internal auditing related to information security.
This involves information security audits of each business division from a perspective that is completely independent of business procedures. Results of audits are relayed to the Information Security Office, and improvements or reviews of systems or activities are implemented whenever required.

Reporting

The NTT DATA Group identifies all customers, shareholders and investors, clients, and employees and their families as stakeholders, and discloses the appropriate information at the appropriate time to fulfill its role of social responsibility as a quality corporate citizen.
The needs of shareholders and investors are carefully attended to by the Investor Relations and Finance Office, the general public, and employees and their families are informed with mass communication via the Public Relations Department, and customers carefully attended to by employees within the Sales Department.
The NTT DATA Group considers taking proactive efforts for establishing information security as one form of social responsibility, and the first information security report as a system integrator was created and released in 2008 to stakeholders.

Backups

NTTDATA-CERT

Established in the Research and Development Headquarters and operates as the Special NTT DATA Group Security Incident Response Team (CSIRT)*
Collects and analyzes information, and devises the appropriate response for preventing security incidents from occurring. Provides emergency response in the event that a security incident does occur.

* Note: CSIRT (Computer Security Incident Response Team) is an incident response team comprised of security specialists. The team collects and analyzes information on security incidents, security-related technologies and vulnerabilities, and conducts activities for effective response and training.

Review of details outlined in the 2010 Information Security Report

Reports for all stakeholders

NTT DATA released Japan's first information security report as a system integrator in 2008. This report is the third time it has been released.
The 2010 Information Security Report outlines the results of implemented initiatives for information security strategies disclosed to stakeholders by NTT DATA.

Efforts raised in the Information Security Report

All initiatives for information security strategies outlined in the previous Information Security Report were achieved.

■Three information security strategies and implementation reports

Information Security Strategies	Implementation Results
Strategy 1 Information security implementation activities for globalization and expanding the group	A monitoring system, training system and internal auditing system for the entire group was established. A multilingual (Japanese, Chinese, English) web interface has been developed for group-wide security training. The training has been completed by 20,536 employees from 83 companies worldwide. To improve the internal auditing system, GSP internal auditor training, which was original only available as classroom training, was also made available in a multilingual (Japanese, Chinese, English) offline training format that can be completed by employees at their desks. Training was provided for 219 new auditors at 66 companies worldwide as a result. Group training and other training sessions were also provided at individual group companies overseas in Chinese, Thai and Vietnamese.
Strategy 2 Establishing procedures for ensuring basic activities to prevent incidents	The "7 Wise Conditions for Basic Security Activities" have been defined, activity checkpoints outlined and unveiled throughout the group. Procedures have also been outlined in the "Initial Response Guidelines for Information Security Incidents" with the aim of ensuring that the entire workplace takes the appropriate steps to respond swiftly to minimize the impact on customers and NTT DATA in the event that an information security incident does occur. Information Security Office and NTTDATA-CERT members also participated in the story-based NTT Group incident response training, covering the steps required from when an information security incident occurs, to obtaining a better understanding of subsequent conditions.
Strategy 3 Information security minded training designed for professionals dealing with information	The "Information Security Improvement Month" is run once per year, and every Friday has been set as "Secure Friday". Posters related to information security are distributed during the Improvement Month. Secure Friday calls for greeting others and announcements broadcast throughout the head office building as a means of raising awareness of information security activities. Personal Information Protection IBT (e-learning) is provided for all employees, and Personal Information Rights Protection Training (classroom training) is organized to cover aspects related to personal information.

NTT DATA Information Security Strategies

NTT DATA has defined information security strategies for achieving management policies and minimizing information security risks.

Specific action plans have been established and implemented based on information security strategies.

Risks surrounding management policies and business management

NTT DATA defines management policies for achieving the "No. 1 level of customer satisfaction" as part of the leading innovation company.
More specifically, the following three priority policies were raised as part of the medium-term management policy announced in FY2009.

- Better capabilities for providing services
- Expanding and improving group business
- Encouraging more environment-oriented management

Risks related to information security are deemed the risks with the potential for the greatest impact on business management in the medium-term management policy.
The various impacts of information security incidents, including the release or leakage of information are considered the greatest risk, and NTT DATA has focused on guaranteeing information security and protecting personal information as a company that provides information systems.

NTT DATA Information Security Strategies

To better respond to the increasing globalization of customers, the NTT DATA Group has also implemented global management to ensure the spread of knowledge to each and every employee of group companies, and to create a work environment that allows the expertise of the entire group to be applied in full.
The objectives of the NTT DATA Group Security Policy (GSP), ensuring safety of information and actively utilizing and sharing information, are essential as a partner that supports customer reform. More specifically, ensuring the safe distribution of knowledge on a global scale, and implementing efforts for preventing incidents related to information security from occurring are essential for stopping the leakage or release of customer's valuable information.
Each and every employee of the NTT DATA Group is aware of their position as professionals dealing with information, and ensures that information security is always of the highest priority when taking actions.
NTT DATA raised the following three information security strategies in FY2011, and has implemented the necessary measures to achieve them.

Information Security Strategies (Objective)

1. Make improvements to information security at group companies located overseas
2. Ensure that basic security activities are conducted
3. Security that contributes to management

Adoption of Information Security Implementation Policies

Action plans based on information security strategies

NTT DATA's information security policies are developed and implemented in accordance with information security strategies. This page outlines specific action plans for each priority topic raised as part of information security strategies.

Make improvements to information security at group companies located overseas

It is vital for the entire NTT DATA Group to share information in as safe a way a possible to achieve the "No. 1 level of customer satisfaction" raised in the management policy.
With this in mind, a security policy has been developed for all group companies, located both in Japan and overseas, that complies GSP, to implement various information security policies. NTT DATA provides the necessary support for ensuring that group companies apply these policies.

■ **Information security objectives:** the objectives of FY2010 was to provide support for developing policies, training and operation for new group companies. The objectives of FY2011 were to improve levels of support provided to group companies located overseas that still had trouble adopting and managing rules, and to conduct monitoring for overseas group companies.
■ **Action plan:** resolve issues by providing support for management, training (literacy, GSP, auditors), caravans and other methods

Ensure that basic security activities are conducted

Preventing incidents related to information security can be resolved with hardware, software and other types of technology, however in the end, the appropriate procedures must be taken by the people using the system.
Existing training and educational policies are constantly reviewed and updated to ensure that each and every employee follows the appropriate procedures. Efforts have also designed for the executive level to ensure that these basic activities filter throughout the entire group.

■ **Information security objectives:** the objectives for FY2010 were to develop the "7 Wise Conditions for Basic Security Activities", set IBT training related to personal information protection, and hold training classes designed for all employees.
The objectives of FY2011 were to ensure better visualization of security levels to ensure that these basic activities also apply to the executive level.
■ **Action plan:** develop and provide education for the "7 Wise Conditions for Basic Security Activities", utilize Information Security Improvement Month and Secure Friday to increase awareness, create advisory reports for the executive level, and organize caravans

Security that contributes to management

From an information security perspective, the uptake of new technologies and new business tools pose new types of risks. NTT DATA carefully studies the impact on convenience that these new technologies and business tools have as a way of minimize these types of risks.
Incidents related to information security can pose a major risk for management for companies. The framework adopted by NTT DATA is designed to prevent incidents from occurring, and minimize damage in the event that an incident does occur.

■ **Information security objectives:** the objectives of FY2010 were to develop usage rules for smartphones and tablet devices, and to establish an incident response team. The objectives of FY2011 were to develop usage rules for social networking services (SNS), and to improve response capabilities during incidents.
■ **Action plan:** develop usage rules for SNS, and smartphones and tablet devices, establish NTTDATA-CERT and join FIRST (*)

* Note: FIRST (Forum of Incident Response and Security Teams) is a community comprised of security specialists from approximately 250 government and private corporate organizations in 50 countries, with the aim of sharing various best practices. (http://www.first.org/)

Auditing, monitoring

NTT DATA auditing and monitoring system

Internal Audit Department

Auditing details	Conducts information security audits of business departments and group companies.

Information Security Office

Monitoring details	Management objectives have been set for each information security activity, including operating conditions of technical measures, state of establishment of information management systems, and operating conditions of personal information protection. Management conditions are monitored and reported to the CISO. Monitoring of group companies has been expanded from 2011 to cover companies located overseas. The CISO then uses various monitoring results to determine whether information security strategies are being used to achieve management policies, and whether contributions are being made to minimize information security risks.

Improvements to policies based on audit results

Information security audits conducted by NTT DATA are designed to check compliance conditions of information security policies and other regulations. Various types of proposals are also provided to make improvements to activities based on audit results.

Within NTT DATA

■ Audit results

- Management was identified as not complying thoroughly enough with information security policies and other relevant regulations.

■ Proposals

- Management requires further compliance with regulations.

■ Implementing improvements

- The Information Security Committee decided to implement "Ensure that basic security activities are conducted" as part of priority activities to raise awareness of information security.
- The degree of penetration of information security within each organization is assessed and an Advisory Report created based on various monitoring results conducted until now. This is used to provide explanations to the executive level of organizations with a low degree of penetration. In addition to the existing bottom-up approach for raising awareness, a top-down approach is also required for raising awareness of information security.

Group Companies

■ Audit results

- Certain group companies located overseas were identified as not having developed their own information security policies that comply with the Group Security Policy (GSP).
- Management was identified as not complying properly with information security policies and other regulations. Group companies located overseas were found to have a large number of errors than group companies in Japan.

■ Proposals

- Positive improvements are required for group companies located overseas.

■ Implementing improvements

- The "Monitoring of Information Security Operating Conditions" (conducted once per quarter) that was not normally conducted for group companies located overseas was also implemented at these companies. This helps to better understand information security operating conditions, and allows improvements to be made.
- To better train employees conducting this monitoring, "GSP Internal Auditor Training" is now conducted in three languages, Japanese, English and Chinese, as part of training for GSP Internal Auditors at group companies located overseas.
- Instead of only Japanese and English, GSP training is now available in Japanese, English and Chinese.

Information security activity case study 1

Make improvements to information security at group companies located overseas

The NTT DATA Group has developed based on the vision of becoming a "Global IT Innovator". This page outlines information security activities that NTT DATA is conducted as part of efforts to expand the group and promote globalization. Various improvements have been implemented for information security, particularly throughout group companies located overseas in FY2011.

PDCA Double Loop

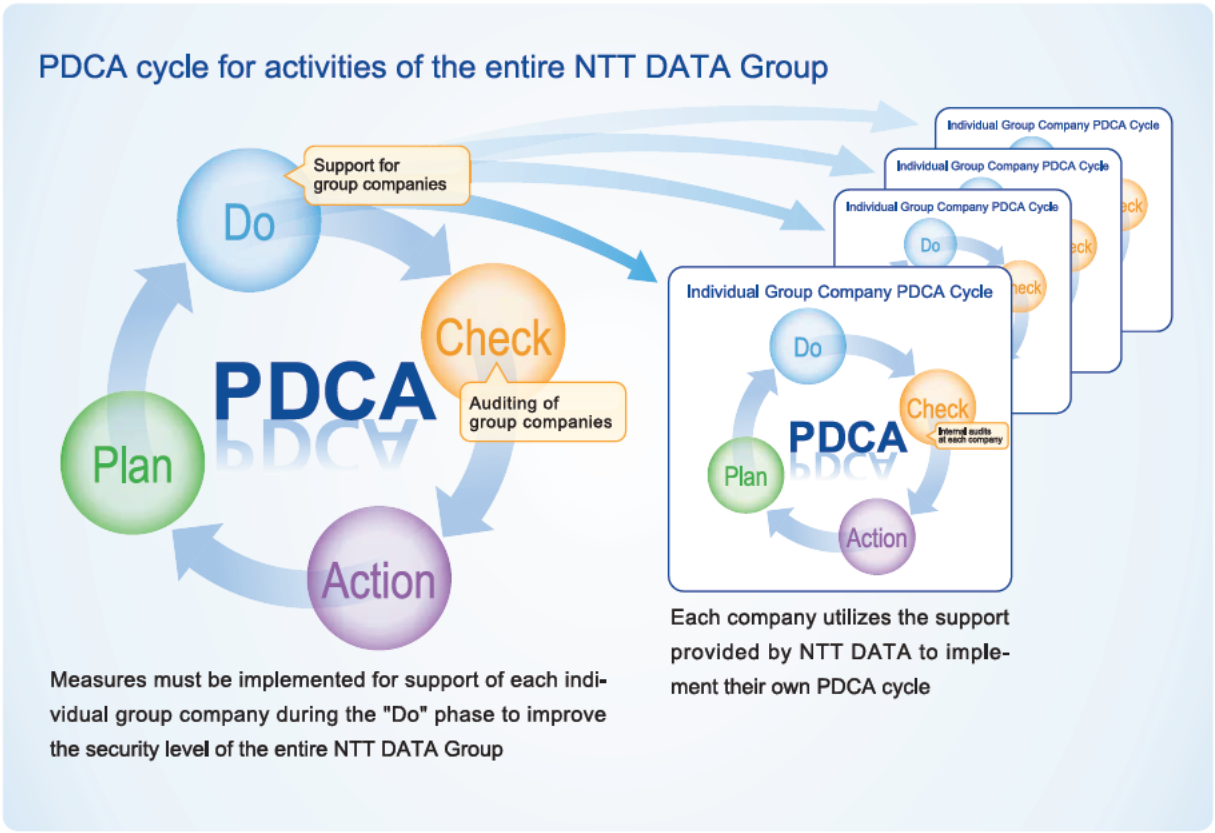
The NTT DATA has adopted two different approaches for the management cycle for information security promotion activities:

(1) Management of the entire corporate group
(2) Individual management by each group company

The ideal balance between these two is when they affect one another in a positive manner. NTT DATA refers to this as the "PDCA Double Loop".

Work focused on "establishing the PDCA Double Loop" until FY2010, with the main objective for the three years from FY2011 focusing on "maturing the PDCA Double Group". Action plans are currently being examined based on this objective. Extra support is provided for group companies located overseas so that they can develop their own PDCA loop faster.

■Example of PDCA cycle implemented within an individual company, while the entire group PDCA cycle is operating



Measures must be implemented for support of each individual group company during the "Do" phase to improve the security level of the entire NTT DATA Group

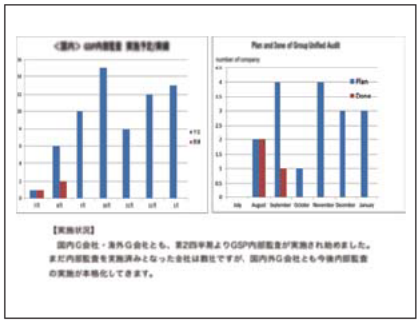
Each company utilizes the support provided by NTT DATA to implement their own PDCA cycle

Priority activities for establishing standard PDCA cycles for the entire group

■Visualization of information security implementation conditions throughout the entire group (group company monitoring)

To better understand the information security level of each group company and propose improvements, NTT DATA monitors the state of establishment and training of information security management systems, and implementation conditions of internal auditing. This monitoring also applied to group companies located overseas from 2011.
Monitoring results are analyzed, and feedback provided to each company. These results allow each group company to better identify conditions throughout the entire company and the level at their own company in an objective manner, and apply appropriate changes to their own activities.
Monitoring results are also a valuable source of information for assessing the effectiveness of information security activities conducted throughout the entire NTT DATA Group.

■GSP Internal Audit Plans and Records



Information security implementation PDCA cycle development and operating support measures within each group company

By expanding the activities implemented at group companies in Japan at group companies located overseas, a PDCA cycle for promoting information security can be generated and improved upon throughout the entire group.

■ Group company caravan

- Members from the NTT DATA Information Security Office actually travel to each group company and conduct interviews to identify the problems and issues that the group company is experiencing. The appropriate advice can be provided and other measures considered there and then.
- This system was used for 4 companies in Japan, and 5 companies overseas in FY2010, and 5 companies in Japan, and 8 companies overseas in FY2011.

■ Information security training for group companies

- The web interface for the group-standard GSP training system is used by the entire group.
- Training is available in three languages, Japanese, English and Chinese, to suit globalization efforts.
- Partners of each group company have also participated in the training program from FY2011.
- In FY2010, the system was used to train employees at 60 companies in Japan and 7 companies overseas. In FY2011, the system was used to train employees at 61 companies in Japan and 22 companies overseas, and also used by 34 companies as part of training for partners.

■ GSP Internal Auditor Training

- Training is provided for employees in charge of actually conducting internal audits at group companies.
- Training focuses on the level of compliance with GSP standard group rules, and involves organizing simulated audits to make conducting audits within group companies easier.
- Training is available in Japanese, English and Chinese from 2011 to suit globalization efforts.
- 169 employees from 57 companies in Japan received training in FY2010, and 268 employees from 66 companies in both Japan and overseas received training in FY2011 to become internal auditors.

■ Information Security Promotion Officer Training

- Meetings are held regularly so that Information Security Promotion Officer of group companies can gather (only in Japan) to learn about best practices of each individual group company, provide explanations on efforts and activities taken by NTT DATA , and share information such as points related to implementing information security.
- This training helps to improve the skills of Information Security Promotion Officers, while being able to share knowledge within the group.
- Meetings have been held twice in FY2010 and FY2011.

Information security activity case study 2

Ensure that basic security activities are conducted

As people dealing with essential information, it is vital to raise awareness to prevent the leakage or release of information.
NTT DATA places a focus on information security training and educational activities to ensure that each and every employee always takes the most appropriate actions, backed with the awareness required of IT professionals bearing the responsibility of dealing with this valuable information.
Extra focus has been placed on the "7 Wise Conditions for Basic Security Activities", established as priority actions developed and implemented from FY2010 onwards.
This page outlines the efforts taken for information security training and educational activities that have been planned and implemented in FY2010 and FY2011.

Development of 7 Wise Conditions for Basic Security Activities and Secure Friday

From FY2009, NTT DATA assigned each Friday as "Secure Friday" as part of essential educational activities for putting information security into practice.
The "7 Wise Conditions for Basic Security Activities" system was established in July 2010 to make these essential activities easier to understand and better known. Each condition was developed over a specific period of time. Educational materials and checklists, case studies and other information were provided when deploying these conditions, so that they could be incorporated into the workplace as quick as possible.

Until September 2011, each and every employee arriving at the NTT DATA head office took part in greeting others on Fridays to spread word of the "7 Wise Conditions for Basic Security Activities".
From October 2011 onwards, trainings involving case studies were held once every quarter based on close call incidents within the company. The "Information Security Workshop" service (more information provided later) has been established for raising awareness of information security.

Information Security Improvement Month

November was assigned as "Information Security Improvement Month" from FY2008. A variety of tools and activities were implemented with the aim of raising the level of information security at the NTT DATA workplace. This provided employees and partners with an opportunity to experience information security and encourage further positive action.
Posters calling for greater information security based on the "7 Wise Conditions for Basic Security Activities" were created in FY2010 and distributed to each workplace, together with other tools designed to promote information security.
Training for countering targeted attacks, and new promotional tools based on the topic of "Only you are in charge of protecting confidential information!" are planned to be conducted and distributed in February FY2011 that the "Information Security Month" is run by the National Information Security Center (NISC).

Examples of information security promotional tools

■Stamps for identifying the type of information

Stamps are distributed to simplify work required for identifying the type of information on the back of the document.

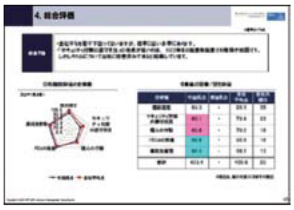
■Information security arm band

Distributed to be worn when information security implementation activities are being conducted. Also worn when greeting others.

Development of Advisory Reports

"Advisory Reports" have been created from FY2011 for each department within companies, and for each group company to ensure that the executive level are fully aware of the security level within their own organization and to be able to devise effective response measures.
Caravans are provided for the executive level and Information Security Promotion Officers at organizations and group companies identified as requiring further advice, and feedback provided through Advisory Reports.
Ideas on potential security risks and methods for improvements are exchanged using the caravans, and more information on the "Information Security Workshop" (more information provided later) is provided as part of suggestions for conducting more detailed measures for improving security.

■Example Advisory Reports



■Overview of Caravans

Information Security Workshop

From FY2011, a new "Information Security Workshop" has been run to highlight actual close call examples and case studies based on the "7 Wise Conditions for Basic Security Activities" to provide a venue for employees to think more carefully about their actions.
The workshop focuses on discussing courses of action taken when responding to problems that have occurred. By examining rules and basic actions together, employees can acquire the knowledge required to deal with these situations.
Examples of actual close calls from organizations that have submitted applications for the workshop are used as case studies to give participants a greater sense of reality. This allows them to delve deeper into discussions, and increase the effectiveness of the workshop.

■Overview of Information Security Workshop

Information security activity case study 3

Security that contributes to management

Measures designed for information security must be implemented as soon as possible for technology and products that are progressing at a phenomenal rate. New technology and products lead to a more convenient social lifestyle, however may also introduce new threats if they are used incorrectly.
NTT DATA has developed an environment to ensure that the business opportunities afforded by these new technologies and products can be utilized quickly and safely. Incidents related to information security can pose a major risk for management. The framework adopted by NTT DATA is designed to prevent incidents from occurring, and minimize damage.
This page outlines the response required to address these new technologies and products, and the efforts taken by the Security Incident Response Team (CSIRT).

Response to smartphones and tablet devices

While the popularity of new products such as smartphones and tablet devices give users greater convenience compared to older cell phones and laptop computers, this higher degree of flexibility comes with a higher risk of information leakage.
NTT DATA has taken the following measures for smartphones and tablet devices to reduce the risk of information leakage.

Response to smartphones

Smartphones differ to ordinary phones in a number of ways.

- Information can be used by accessed them via various applications (a high possibility that information is stored using cloud services)
- A globally common OS is generally used, which opens it up to potential risk from virus

To address this situation, NTT DATA has introduced a system from May 2011 that utilizes a special service to ensure that information does not remain on the device or on cloud services when using a smartphone to access company servers.
This approach ensures that company email or other company systems can be used safely from outside the company network.
Options are also available that outline in detail using guidelines the settings required for security functions so that the essential security measures can be set properly.

Response to tablet devices

Tablet devices are easier to use and more portable than conventional laptop PCs, and have increased in use within the business scene. Yet as tablets are unable to use the thin client framework developed by NTT DATA, ensuring that these devices can be used with the same level of safety as smartphones and laptop PCs remains a challenge.
To address this issue, rules have been established for device settings and usage procedures. Models that comply with these rules have been accepted under the same usage conditions as thin clients on an application-basis from November 2010.
These rules will continue to be reviewed, and the number of accepted models increased as NTT DATA services and the functions of the models themselves continue to advance.

Responding to social media

Until recently, social media was generally used separately by each individual, however as companies are also able to create accounts these days, social media is increasingly used as a promotional tool for business.
NTT DATA released its "Social Media Policy" in June 2011 to cover social media that is used by companies for official purposes. This policy outlines NTT DATA's core approach to dealing with social media. NTT DATA operating rules were also developed around the same time, and accounts run by companies are required to adhere to this social media policy. An approach to managing all company accounts has been taken and released as the "List of Social Media Official Accounts".

NTT DATA Social Media Policy: http://www.nttdata.co.jp/info/privacy-sm.html
NTT DATA Social Media Official Accounts: http://www.nttdata.co.jp/info/accountlist.html

NTTDATA-CERT responding to incidents

IT services and related functions continue to progress rapidly, which has increased the complexity and diversity of attacks. To combat these so-called cyber attacks, companies need to acquire any relevant information as soon as possible and devise the appropriate countermeasures. If the appropriate steps are not taken, and there is an incident related to information security involving personal information being leaked, the negative brand image will result in customers looking for different, safer alternatives, which poses a major risk for management.
To provide systems and services safely and with complete peace of mind to customers in response to management risks related to information security, NTT DATA established "NTTDATA-CERT" in July 2010. This system is comprised of the Security Incident Response Team (CSIRT) for preventing security incidents from occurring, and responding swiftly and appropriately in the event of emergencies when incidents do occur.
NTTDATA-CERT is working to establish a global communication path with other CSIRT organizations as a way of improving its response capabilities in times of incidents.

The system is designed so that NTTDATA-CERT and employees in the related departments work together to address the situation in the most appropriate manner if an information security incident occurs within NTT DATA and the NTT DATA Group.
To ensure that the appropriate response can be taken in the event that an information security incident does occur, NTTDATA-CERT joined in story-based incident response training covering the actual timeline of information security incidents at NTT Group from the point they occurred, to when conditions were identified.

■Image of incident response training conducted at NTT Group

Security in line with social conditions

Business continuity following the Great East Japan Earthquake and efforts to deal with summer power restrictions

NTT DATA was not damaged to an extent following the Great East Japan Earthquake where business could not be continued.
A disaster response task force was established on March 11, the day that the Great East Japan Earthquake struck, to check the safety of employees and their families, and to confirm any damage to company buildings. Efforts were also taken to restore and maintain services of customer systems in areas affected by the disaster.
Power conservation efforts were also introduced between July 1 and September 22, 2011, in response to requests from the government to reduce power consumption within the area covered by Tokyo Electric Power Company (TEPCO) during the summer of 2011.
This page outlines the efforts taken for power conservation, and in particular the steps taken for information security.

1. Rolling power shutdowns throughout office floors

A schedule for shutting down air-conditioning, lighting and power outlets on certain days was developed for the head office (Toyosu Center Building, Toyosu Center Building Annex) and each office floor as a means of minimizing power consumption.
A "shared office" was established within the head office building to ensure that a certain portion of employees working in offices on floors without power were still able to work when they arrived at the office. The shared office only allowed thin client terminals to be used, which helped to ensure security levels, while also being available for employees from various departments.

2. Reforms to work

NTT DATA has taken a pro-active approach to work by implement reforms such as introducing teleworking, encouraging employees to take more holidays, and changing the actual day of holidays every week.
Telework requires that the same information security policies as ordinary work are adhered to, and that employees comply with the following major rules related to technical aspects and operational aspects to maintain security.

■ Technical aspects

- In general, use thin client PCs loaned by the company
- One-time password used for remote access certification
- If wireless LAN networks are used at employee's homes, network encryption is required

■ Operational aspects

- Confirmation of security rule checklists when applications are submitted for work-at-home
- Prohibit work using personal information or highly confidential information
- Prohibit use of printed media at home
- Prohibit use of faxes at home
- Ensure methods to prevent family from approach the work area during work-at-home

3. Power conservation by replacing PCs

NTT DATA replaced approximately 10,000 desktop PCs used within its offices to low power consumption laptop PCs or thin client terminals.
A guide manual and checklist was created for individual settings of new laptop PCs to prevent employees forgetting to configure the appropriate settings for information security.

The data contained within the old desktop PCs was erased securely, before the PCs themselves were recycled. When PCs were donated to areas affected by the disaster, rules were created to ensure that they could be used safely and to prevent leakage of information.

Response to cyber attacks

Reports of leakages of personal information following cyber attacks by hacker groups on Japanese companies in America, and targeted attacks on companies and other organizations in Japan were covered widely by the mass media throughout 2011.
Ensuring that systems are completely secure is one approach to prevent cyber attacks. Since 1998, NTT DATA has focused on identifying security vulnerabilities in hardware and software considered essential for system development and operation of NTT DATA, and has been releasing appropriate security patches. A vast amount of different information is always collected, summarized, and released as email magazines on the day the information became available, or provided via the company website. This enables employees in charge of system development and operation to identify security vulnerabilities in a more centralized manner, and obtain information required for deploying security patches. Sources for this email magazine and website updates are based on NTTDATA-CERT's very own information network.
In May 2011, the NTT DATA Group also conducting thorough reviews of web systems used for accessing personal information.

■Image of the security information email magazine

Improving understanding and awareness of information security

Continuous information security training and education

The NTT DATA Group is aware that each and every executive, employee and partner is a professional dealing with information, and always considers information security policies during daily actions to ensure continuing information security.
NTT DATA focuses on improving understanding of rules and actions, and takes the appropriate steps for employees to develop an information security-minded approach required for work by adopting ongoing information security training and educational activities.

Information Security Training

The NTT DATA Group has conducted ongoing information security training to ensure that employees gain an understanding of the need for the protection of personal information and rules outlining group security policies, as well as ensuring that they act with a full awareness of information security.

■ Information security training records at NTT DATA in FY2010 and FY2011

Applicable to	Type of Training	Details, Objectives
All employees (required)	Personal information protection IBT (Web interface)	Approach to personal information / Methods for dealing with personal information / Understanding the details of company regulations / Increasing awareness of personal information * Records for FY2010, FY2011: employees 100%
	Information Security Policy Assessment (Web interface)	Increasing awareness of information security policies / Understanding of basic actions in the event of an information security incident / Dealing appropriately with cell phones and small portable media etc, acquiring correct knowledge * Records for FY2010, FY2011: executives, employees 100%
Specific projects	Personal information rights protection training (classroom training)	Training to understand the steps required if personal information is acquired during the course of a project * Records for FY2010: 5 times, 140 employees, FY2011: 4 times, 83 employees
All employees (optional)	Information Security Workshop	Workshop designed around the items that receive a large number of inquiries related to information security and protection of personal information * Records for FY2011: 5 times (including those planned to the end of the year)
All employees (per work group, optional)	Case study for "7 Wise Conditions for Basic Security Activities" (case study)	A group discussion focusing on thinking for yourself for gaining a better understanding and penetration of information security policies Conducted at each workplace with the topic in line with "7 Wise Conditions for Basic Security Activities" conducted every two months
Each management level	Information Security Course (classroom training)	Description of the knowledge, differences in roles and responsibilities, approach, and required items for each employment position, including new employees, mid-career employees, division managers, and department managers Acquiring knowledge for improving understanding and implementation of information security
Partners (required)	Personal Information Protection In troduction Training Information Security Training (Web interface, provision of training materials)	Provides training of content that should be known by partners working at NTT DATA related to the protection of personal information, and information security rules at NTT DATA Training is required when using company systems, and regularly training is essential * Available in multilingual format (English, Japanese, Chinese)
Partners (new)	Information Security Training Handbook	Handbook that outlines how to deal with information security and personal information when working within the NTT DATA, distributed by contract from the NTT DATA Group. The handbook is for new NTT DATA Group partners. * Available in multilingual format (English, Japanese, Chinese)

Supporting group company educational activities

NTT DATA provides the required tools and support required by each group company to develop their own information security training with a view of improving the level of information security throughout the entire group, and to apply the "PDCA Double Loop" concept designed specifically with globalization and group expansion in mind.

Group company training support tool

Applicable to	Type of Training	Details, Objectives
Group Company Employees	GSP security training (Web interface)	Improving NTT DATA Group Security Policy understanding / Methods to deal with personal information / Description of the NTT DATA Group Security Policy * Available in multilingual format (English, Japanese, Chinese) * Records for FY2010: 60 companies, 14,197 employees, FY2011: 83 companies, 20,536 employees
Group Company Partners	GSP Security Training for partners (Web interface)	Approach related to personal information protection, training for information security rules that should be known as new NTT DATA Group partners * Started in FY2011: 34 companies, 4,752 employees
Internal Auditors	GSP Internal Auditor Training (intensive class training, also available in format that can be completed by employees at their desks from FY2011)	Training for conducting information security audits Training with simulated audits * Available in a multilingual (English, Chinese, Japanese) format that can be completed by employees at their desks * Records for FY2010: 57 companies, 169 employees, FY2011: 66 companies, 268 employees (including overseas companies)

Examples of information security promotional tools

In addition to focusing on the basic security activities that have been raised as priority topics as part of information security strategies, NTT DATA also conducts ongoing information security educational activities with the aim of maintain and increasing the level of information security.

Information security promotional posters

Posters are designed on recent topics such as world and social trends and priority topics of information security strategies, and help to better identify information security within each workplace. A multilingual version started being issued from FY2008 and is released to other group companies.

Topic for FY2010
Security is your lifeline
Incident Zero
(multilingual)

Topic for FY2011
Thin client usage promotion / Recheck PC settings / Prevent sending by mistake / Cautions when using SNS
(multilingual)

Monthly newsletter "Security Today"

Outlines the efforts taken within the NTT DATA Group for information security, social condition related to security, the most recent technology, and reports of incidents in an email magazine that is published monthly.
Part of the newsletter is provided to group companies and partners to share information.

Message from CISO

From FY2011, CISO will be sending messages directly to employees once per quarter. This can be used as an opportunity for CISO and employees to interact, via reports on the latest trends, approaches taken by CISO, and requests for employees.

Efforts taken by contractors

NTT DATA has developed various standards to prevent the unexpected leakage or release of information from partner companies contracted to develop software. When contracting work that deals with confidential information or personal information, declarations are received, and checks conducted of security response conditions being taken.

Partner company selection

Checks of system and response conditions	To select clients that meet certain standards, a different set of standards is defined and the client interviewed to check their current security response conditions.
Present rules, agree on response rules	Present rules related to security management and protection of personal information required for a particular project, and reach an agreement on the level of response required by the partner company.

Efforts after business contracts

Start contract

Training, check declarations	· Provide training to partner companies dealing with information in line with the details agreed upon during the contract. · Check and receive copy of declarations.
Report from partner company	Information management systems, conditions for dealing with information, and security response conditions are checked regularly using submitted reports or meetings that are held.
Audit of partner company	On-site or other inspections may be conducted if required to check security response conditions, and to determine whether information is being operated and managed appropriately. Requests for corrections or improvements may be issued depending on the results.
Check of information disposal	Information that is no longer required for its original purpose, information that is in use but no longer required, or media storing this type of information must be returned or destroyed using the methods stipulated in advance by the project.

End contract

Information security incident occurrence conditions

NTT DATA has not been subjected to any major information security incidents between issuing the first Information Security Report in 2008, and this report.

- Introduction of PCs for information leakage prevention solutions (Total Security Fort: TSF)
- In general, all PCs taken out of the company are thin client terminals

The following technical measures are implemented within NTT DATA to prevent unexpected major information security incidents from occurring.

- Introduction of email filtering solutions
- Introduction of Web (URL) filtering solutions
- Anti-virus software installed on computers used throughout the company

Third party assessments, certification

IMSM certification acquisition conditions

Where required, NTT DATA and NTT DATA Group companies have acquired international standard ISMS (ISO/IEC 27001) certification for information security management system when dealing with confidential information or personal information.

Group companies with organizations that have acquired ISMS certification are as follows.
(40 companies including NTT DATA, as of the end of December 2011)

Companies with groups that have acquired ISMS Certification

NTT DATA Corporation	NTT DATA INSTITUTE OF MANAGEMENT CONSULTING, Inc.	QUNIE Corporation
NTT DATA SYSTEM TECHNOLOGIES Inc.	NTT DATA SMS Corporation	NTT DATA SEKISUI SYSTEMS Corporation
NTT DATA i Corporation	NTTDATA CUSTOMER SERVICE Corporation	Technology Power Corporation
NTT DATA INTELLILINK Corporation	NTT DATA FORCE CO., LTD.	EMAS Co.,Ltd
NTT DATA FINANCIAL CORE Corporation	NTT DATA FRONTIER Corporation	NTT DATA TERANOS Corporation
NTT DATA HOKKAIDO Corporation	Nihon Card Processing Co., Ltd.	NTT DATA NCB Corporation
NTT DATA TOHOKU Corporation	Realize Corporation	NTT DATA Getronics Corporation
NTT DATA SHINETSU Corporation	NTT DATA 3C Corporation	NTT DATA CCS Corporation
NTT DATA TOKAI Corporation	NTT DATA WAVE Corporation	NTT DATA MSE Corporation
NTTDATA HOKURIKU Corporation	e-OSAKA INTERNET DATACENTER	JSOL Corporation
NTT DATA KANSAI Corporation	NTT DATA CHINA OUTSOURCING Corporation	NTT DATA ITECS Corporation
NTT DATA CHUGOKU Corporation	NTT DATA BUSINESS BRAINS Corporation	NJK Corporation
NTTDATA SHIKOKU Corporation	NTT DATA SOLFIS Corporation	NTT DATA MCS Corporation
NTT DATA KYUSHU Corporation		

Privacy Mark Grants

Companies under NTT DATA or the NTT DATA Group that have been granted the Privacy Mark are as follows.
(32 companies including NTT DATA, as of the end of December 2011)

Group companies granted with a Privacy Mark

NTT DATA Corporation	NTT DATA SMS Corporation	NTT DATA ABIC Co., Ltd.	NTT DATA TERANOS Corporation
NTT DATA INTELLILINK Corporation	NTTDATA CUSTOMER SERVICE Corporation	NTT DATA SOLFIS Corporation	NTT DATA CCS Corporation
NTT DATA HOKKAIDO Corporation	NTT DATA MANAGEMENT SERVICE Corporation	NTT DATA BUSINESS SYSTEMS Corporation	JSOL Corporation
NTT DATA TOHOKU Corporation	NTT DATA FRONTIER Corporation	NTT DATA SEKISUI SYSTEMS Corporation	XNET Corporation
NTT DATA TOKAI Corporation	Nihon Card Processing Co., Ltd.	NTT DATA SMIS CO., Ltd.	NTT DATA ITECS Corporation
NTT DATA KANSAI Corporation	NTT DATA UNIVERSITY Corporation	NTT DATA ENGINEERING SYSTEMS Corporation	TOUHOKU INFORMATION SYSTEM CO.,LTD.
NTT DATA CHUGOKU Corporation	NTT DATA 3C Corporation	Technology Power Corporation	Media Drive Corporation
NTT DATA INSTITUTE OF MANAGEMENT CONSULTING, Inc.	NTT DATA-R Corporation	Comet Information Co., Ltd.	EMAS Co., Ltd

Information security activity timeline

Social Developments

1995
Part 1 of British Standard BS7799 Information Security Management developed

1998
Part 2 of British Standard BS7799 Information Security Management system developed
April Started operation of Privacy Mark from Japan Information Processing Development Corporation (JIPDEC)

1999
May Revised BS7799 Part1 and Part2

2000
July Developed JIS X 5070, the Japanese version of ISO15408 International standards for information security
September BS7799 Part 1 became International Standards ISO/IEC17799

2001
e-Japan strategy developed

2002
April Started operation of the ISMS Conformity Assessment Scheme from Japan Information Processing Development Corporation (JIPDEC)

2003
October Japan Information Security Audit Association established

2004
Google stocks went public

Technical Developments

1994
"DES" decrypted using linear cryptanalysis

Windows 95 went on sale

1996
Yahoo! (Japanese) service started operations
June "Laroux" Microsoft Excel macro virus discovered

1997
"PKI" proposed in America

Google established

NTT Docomo "i-Mode" service started operating
"Napster" announced
March "Melissa" mass-mailing virus spread
April First commercial ADSL service in Japan started

Google (Japanese) started operations
Increase in DoS attacks
October "WinMX" Beta version released
December NTT East and West "Flet's ADSL" started

AES selected as the American government's standard encryption service to replace DES and triple DES
"Code Red" and "Sircam" worms spread
June NTT East and West "B Flet's" started
November First person arrested for using "WinMX"

Botnet appeared
May P2P software "Winny" Beta version released

Skype established
January "Slammer" worm spread
August Skype public Beta version released

January "Share" released
February "W32/Netsky" worm spread
May Developer of P2P software "Winny" arrested

NTT DATA Achievements, Developments

1997
Information Security Committee established

1998
December "Information Security Policy" developed

1999
CISO (Chief Information Security Officer) position established
February IBT (Internet Based Testing) training started

2000
February Greater venture systems (NTT DATA INTRAMART CORPORATION established)
March Accounting system using consolidated balance sheets started from the March quarter
June Information security policy assessments started

2001
February "Standard Security Policy (SSP)" developed
June "Personal Information Protection Regulations" developed
July "Personal Information Protection Policy" announced
September First BS7799 certified in Japan

2002
September Training (CISP) started for partners
October NTT DATA Group Security Agreement (GSA) established

2003
June Acquired Privacy Mark Certification
July Established system for regional subsidiaries (system incorporating nine regional subsidiaries)

Social Developments	Technical Developments		NTT DATA Achievements, Developments
2005 "Web 2.0" became popular **April** Personal Information Protection Law enacted in full	**December** "Youtube" service officially started	2005	**2005** **June** P2P software checks became available for remote connection PCs **November** Started TSF operation
2006 Numerous cases of information leakage reported due to file sharing software "Winny" **February** "Information Security Day" established	"Facebook" released to the public **July** "Twitter" service started operations **December** "Amazon EC2" started, kicking off the cloud computing concept **December** Domestic high-speed PLC products went on sale	2006	**2006** **July** Started trials of Telework **September** Declaration received from all Employees at NTT DATA (ensuring that users delete work related information from their own PCs, and prohibiting work on their own PCs) **October** Declarations required from all Employees working within the NTT DATA Group **November** Declarations required from subcontractors
2007 **January** "Information Security Governance Seminar" held	**October** The number of Skype online users exceeded 10 million people	2007	**2007** **April** ISMI Certification obtained for the head office building **July** Thin client services started **December** Email filtering service started
2008 **January** First person arrested in Japan for creating computer virus **June** National Information Security Center (NISC) released "Secure Japan 2008"	**February** Virus found to spread via USB memory **April** Google and Salesforce.com announced tie-up for cloud computing	2008	**2008** **February** Telework system started **March** First "2008 Information Security Report" as system integrator published **April** NTT DATA Group Security Policy (GSP) published **November** "Information Security Improvement Month" established
2009 **February** NISC released "2nd Information Security Basic Plan" **June** NISC announced "Secure Japan 2009" **September** Personal Information Protection Law shifted to the Consumer Affairs Agency	**April** "Gumblar" botnet appeared	2009	**2009** "Secure Friday" established **December** Comprehensive cloud solution service announced
2010 **July** Information Security Policy Council released "Information Security 2010" **July** Unfair Competition Prevention Act revised **November** Video of Chinese boat collision incident leaked	Widespread attacks targeted Twitter **May** iPad released in Japan **December** First botnet virus "Geinimi" for Android appeared	2010	**2010** **March** "2010 Information Security Report" published **July** "7 Wise Conditions for Basic Security Activities" established **July** NTTDATA-CERT established
2011 **March** Widespread fishing scams reported in the aftermath of the Great East Japan Earthquake **May** Vast amounts of personal information leaked from American subsidiaries of Japanese companies due to cyber attacks **June** "Virus Creation" is criminalized following revisions to criminal law **September** Targeted attacks discovered against the Japanese defense industry	**May** IPv4 addresses depleted in the Asia Pacific region	2011	**2011** **April** Joined NTTDATA-CERT FIRST **May** Internal connection service for smartphones started **June** NTT DATA Social Media Policy announced **July** Office computers switched to notebook PCs following restrictions to power consumption

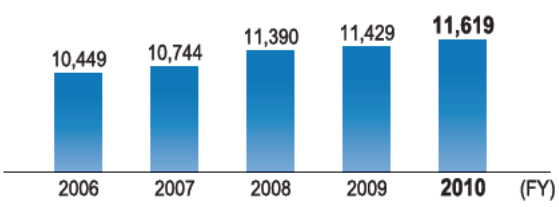
Company overview

Ever since separating from Nippon Telegraph and Telephone Public Corporation in 1988, the NTT DATA Group has been providing information systems and services to address the requirements and issues of society. The company is involved with systems for public services, finance, manufacturing, logistics, communications, medical, health care and other corporate-oriented systems, as well as social infrastructure services that cover multiple industries.

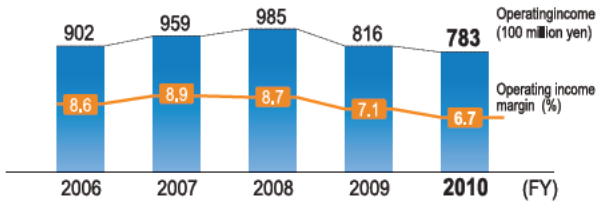
Today, NTT DATA is focusing its resources on globalization, and has expanded its offices located in 143 cities, in 34 countries as of September 30, 2011.
As a company that is truly pioneering the IT industry in Japan, and a company that has a global presence with businesses operating in every region on the planet, there are plans to provide further support to society and develop new frameworks and value required for reforms.

Name	NTT DATA CORPORATION
Head Office	Toyosu Center Building, 3-3, Toyosu 3-chome, Koto-ku, Tokyo 135-6033, Japan
Established	May 23, 1988
President and CEO	Toru Yamashita, President and Chief Executive Officer
Common Stock	142,520 million yen (as of March 31, 2011)
Net Sales (consolidated)	1,161,900 million yen (April 1, 2010 to March 31 2011)
Ordinary Income (consolidated)	78,300 million yen (April 1, 2010 to March 31 2011)
Number of Employees (non-consolidated)	10,139 (as of March 31, 2011)
Number of Employees (consolidated)	49,991 (as of March 31, 2011)
Subsidiaries and affiliated companies	Consolidated subsidiaries: 215 (as of March 31, 2011) Affiliated companies: 20 (as of March 31, 2011)

■Consolidated net sales (units: 100 million yen)



■Group operating income / Group operating income margin



Business Areas	System integration/Networking system services Other business activities related to the above

State of Global Offices

Europe, Middle East, Africa regions
55 cities
6,100 Employees

Asia Pacific region
34 cities
13,400 Employees

North American region
54 cities
7,000 Employees

* No. of Employees as of September 30, 2011

Implementation of information security as a corporate group

In closing

There have been major changes to the environment surrounding corporate information security, and the speed, diversity and extent of damage that these changes can bring about is the real threat today. Some cases that have become major social issues in particular were the 100 million or more cases of leakages of personal information in 2011 arising due to attacks exploiting weaknesses in application servers, or the leakage of confidential information due to targeted attacks. It became clear that companies needed to take further steps against attacks from outside sources. Meanwhile, the uptake of smartphones and tablet devices has increased at a tremendous rate in line with social networking services and cloud computing services. It seems that society has finally entered the post-PC era.

By maintaining an appropriate balance between ensuring safety of information and actively utilizing and sharing information, the NTT DATA Group applies its knowledge throughout the entire group and provides brand new value to customers as part of information security policies.

With this in mind, NTT DATA has been progressing based on three types of information security strategies developed last year. The first is to make improvements to information security at group companies located overseas.

The number of group companies located overseas has increased as the group expands internationally, and NTT DATA is focusing on providing the appropriate support for developing policies, operation and training. The second is ensuring that basic security activities are conducted. To prevent individual employees from causing incidents, NTT DATA has developed the "7 Wise Conditions for Basic Security Activities" that outline the appropriate activities to be taken to raise awareness of information security, and also runs related training and case studies. And the third is security that contributes to management. Rules and guidelines have been developed and managed to ensure that smartphones, tablet devices, social networking services and other tools and services that are so essential to business today can be used safely. Response to incidents has been improved by establishing the special "NTTDATA-CERT" team, in order to prevent incidents related to information security and respond to emergencies.

Information security professionals also address inquiry and suggestions related to information security received from within the company or from other group companies in candidly and in a straightforward manner. While the efforts of this work may not be immediately clear with day-to-day business, addressing each inquiry properly helps to respond swiftly to customers and minimize security risks spreading within the company or to other group companies.

As a result, these efforts serve to increase levels of customer satisfaction and improve information security within the NTT DATA Group.

This report outlined the various steps taken by the NTT DATA Group ranging from information security governance to initiatives deemed to be of significant social concern. It will give me great delight if people who read through this report found it useful in one way or another.

The NTT DATA Group is aware of its position as professionals dealing with information, and always considers information security when taking actions. Implementing this information security governance ensures that customers are always provided with a new sense of value with peace of mind and reliability.

NTT DATA Corporation
Manager, Information Security Office,
Quality Assurance Department
Shigefumi Takahashi

NTT DATA Group Information Security Report 2012
Published by: Information Security Office, NTT DATA CORPORATION

Issue Version 1.0 March 2012

NTT DATA Corporation
Toyosu Center Bldg., 3-3, Toyosu 3-chome,
Koto-ku, Tokyo 135-6033, Japan
Tel: 03-5546 8051 (switchboard)
www.nttdata.com