Governance

Information Security

Stance on Social Issues

Cyber-attacks that threaten corporate management are becoming increasingly diverse and malicious. Their targets are broadening in reach and, irrespective of size or industry, we have entered an era where everyone is a target. For companies and organizations, information security is regarded as an important management task, and we continue to seek further advanced measures to deal with the issue. The Anritsu Group believes that properly handling and protecting information depends on sharing information and setting an equal level of security across both domestic and overseas areas to establish a robust management system.

Policy

In conducting its business activities, the Anritsu Group considers it a social obligation to protect the information of all stakeholders, including customers, shareholders and investors, suppliers, employees, and it also recognizes these information assets as important property. Having established the basic rules of information management from this perspective, we are making a continuous effort to maintain and enhance information security.

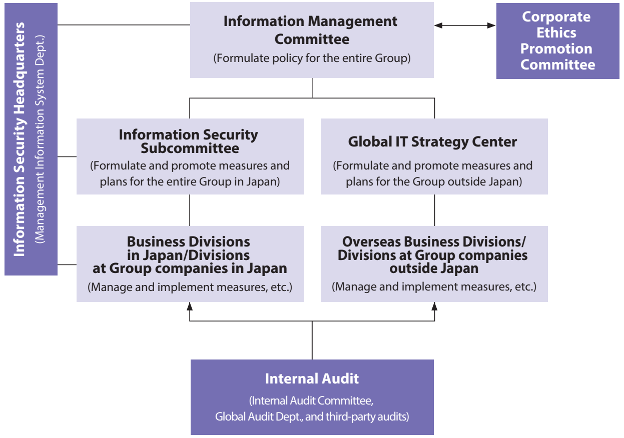
WEB *Basic Rules of Information Management*

Structure

Anritsu has organized an Information Management Committee, made up of key executive officers from each business division and Group companies, to formulate policies on investment and strategies related to information management for the entire Group.

For Domestic Group companies, we established an Information Security Subcommittee operating under the Information Management Committee, which is responsible for conducting policy enactment and implementation measures and activities such as employee training, countermeasures to deal with an incident when it occurs, and information sharing. For overseas Group companies, we established the Global IT Strategy Center, consisting of IT managers of the regional headquarters. The center focuses on strengthening controls over IT, including security, at overseas Group companies.

Information security management system


Information Security Headquarters
(Management Information System Dept.)
Information Management Committee
(Formulate policy for the entire Group)
Corporate Ethics Promotion Committee
Information Security Subcommittee
(Formulate and promote measures and plans for the entire Group in Japan)
Global IT Strategy Center
(Formulate and promote measures and plans for the Group outside Japan)
Business Divisions in Japan/Divisions at Group companies in Japan
(Manage and implement measures, etc.)
Overseas Business Divisions/ Divisions at Group companies outside Japan
(Manage and implement measures, etc.)
Internal Audit
(Internal Audit Committee, Global Audit Dept., and third-party audits)

ISO 27001 Certified Organizations

- Japan: Management Information System Department and CAD Team, Fundamental Technology Department, Engineering Division
- EMEA: Anritsu A/S Service Assurance Business Unit

Goals

▶ Promoting Security Measures Against Intrusion

Cyber-attacks are becoming increasingly diverse and sophisticated, making it virtually impossible to completely prevent them. It is therefore important not only to take measures that prevent intrusion but also to promptly take action to minimize damage in the event of an attack. Going forward, we will continue to promote comprehensive measures that address the situation both before and after an attack.

▶ Building a Robust, Uniform Global Security System

The Anritsu Group, in its global operations, will connect all its offices around the world through a network to further facilitate information sharing. Including TAKASAGO Ltd., acquired through M&A in fiscal 2021, we will promote the establishment of a globally integrated security system.

Activities and Achievements

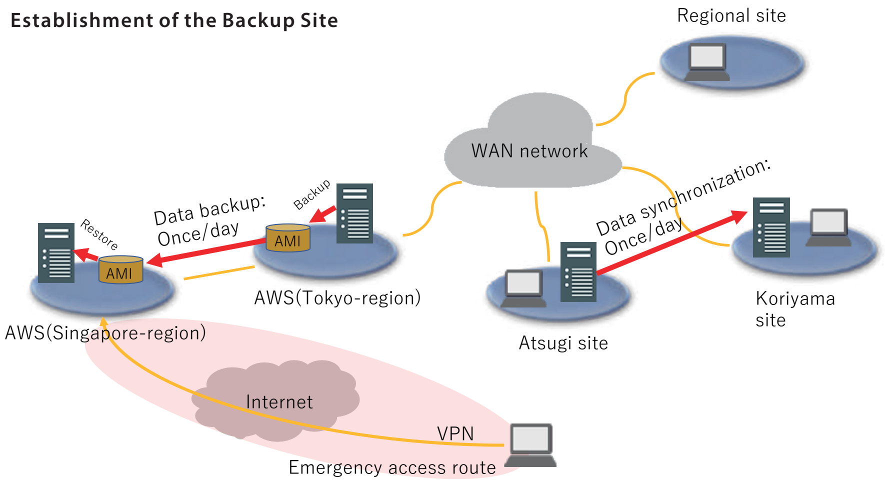
Strengthening Measures against Ransomware

There has been an alarming increase in victims of ransomware attacks in recent years. The manufacturing industry is no exception, as such incidents have affected the entire supply chain after a company has been victimized. It is important to minimize the impact of ransomware on business operations not only by taking general security measures to prevent intrusion but also by quickly detecting and recovering from attacks. For this reason, we must be prepared for such security incidents by considering them as a risk in our BCP. In fiscal 2021, as a countermeasure against ransomware attacks, we built a new backup site to ensure proper system backup and shorter recovery time. With the new backup site, we can minimize the impact of any system failure due to ransomware attacks by starting up the standby system on the site. In addition, recovery time is reduced from one week to one day.

Conducting Employee Training and Phishing Email Drills

Every year, we conduct information security training for all employees online. In fiscal 2021, we conducted training on ransomware threats and handling email. We have also increased the frequency of phishing email drills to every two to three months to raise awareness of cyber-attacks via email.

Establishment of the Backup Site


Regional site
WAN network
Data synchronization: Once/day
Koriyama site
Atsugi site
Backup
AMI
AWS(Tokyo-region)
Data backup: Once/day
Restore
AMI
AWS(Singapore-region)
Internet
VPN
Emergency access route