AUTRANS

Autrans IT Security Policy

Established on April 1, 2015

Email: it@autrans.com

Autrans IT Security Basic Policy

Identifying information security as a critical challenge in our business, Autrans aims for properly preserving, managing, and utilizing valuable information resources. Everyone who uses, creates, and manages the information resources of Autrans should recognize the importance of IT security and observe this policy.

IT Security Management Structure

Autrans

- Compliance Committee
- Compliance Committee/ Information Security Subcommittee
- Department/Division (IT Security Leaders)

Consolidated Subsidiaries (IT Security Leaders)

Coverage/Target

- Coverage
  - Overseas offices including liaison offices/branches
  - Consolidated subsidiaries, except below:
    - Companies without IT environments and/or employees that would be the target of this IT Security Policy (e.g. SPC, holding companies)
    - Listed companies and their affiliated companies
- Target

All executives and employees, including temporary staff and contractors, working at the offices in the coverage list above who utilize information resources of Autrans.

Definition of Information Resources

In this policy, the term "information resources" refers to IT devices, external storage devices/media, information systems, IT environments, and the information itself which has been supplied, lent, or permitted by the company. In specific, it includes stored data, various kinds of IT devices (PCs, servers, iPhones, etc.), external storage devices/media (e.g. USB memory), software, services (email system, the Internet, business application system, etc.), and network environments.

Definition of IT Security

The term "IT security" refers to appropriately utilizing, managing, and protecting information resources to preserve "confidentiality," "integrity," and "availability" (known as the three IT security factors).

- The term "confidentiality" refers to securing the system so that only authorized people can access particular information.
- The term "integrity" refers to securing the system so that data retains its validity, completeness, and accuracy; and is not destroyed, tampered with, or erased.
- The term "availability" refers to ensuring that information and services are readily available to people who need them.

Management Responsibilities

The management of each group company is responsible for carrying out the following tasks in a responsible manner. Depending on the system, all or some of these tasks can be assigned to managers, but management is ultimately responsible for all tasks under all circumstances.

(1) Notifying all applicable personnel within the company about this policy and ensuring that they follow the policy completely

(2) Introducing, modifying, and operating information resources, and appropriately managing the costs associated with these resources

(3) Carrying out system risk management activities for information resources owned by the company, in accordance with the separately specified "System Risk Management Guidelines for Group Companies," especially the following:

1. Annually check each system for any potential risks that may compromise the three IT security factors ("confidentiality," "integrity," and "availability"), taking the importance of each factor into accout. Upon doing so, ensure that appropriate IT security measures have been implemented to counter such risks.
2. Respond to system risks as requested by Autrans and report the implementation status to Autrans Compliance Committee/Information Security Subcommittee.
3. If an incident occurs that compromises any of the three IT security factors, immediately take appropriate measures to minimize damage to the system and inform the Autrans Compliance Committee/Information Security Subcommittee of the incident.

Notes to Users

1. Use of company information resources

(1) Information resources of the company are supplied to its employees for business purposes. Use of information resources of the company for other than business purpose is prohibited unless specifically authorized.

(2) Only information resources supplied or approved by the company are permitted. Privately owned and other externally obtained devices (e.g. PCs , USB memories) should not be utilized and/or connected to the corporate network unless specifically authorized.

(3) All company PCs must have anti-virus software installed.

(4) Use of unauthorized and/or illegally obtained software is strictly forbidden. Make sure that the software applications installed on PCs are officially licensed.

(5) When leaving the work area, users should log off of their PCs or lock it by using a password-protected screen saver and never allow unauthorized parties to use their PCs.

(6) To prevent the loss of critical information, store data in an authorized recoverable fileserver. If data must be stored on a PC, take measures to safeguard it such as backing up the data.

(7) To prevent the loss of sensitive data while using external storage devices/media, take measures against information leakage such as using encrypted devices or password-protection of data files. Note that use of privately owned devices/media as well as privately owned PCs are strictly forbidden unless specifically authorized.

(8) When disposing of information resources (PCs, servers, USB memories, etc.), take steps to prevent leaking sensitive information such as deleting the data in a way that is beyond recovery.

(9) All users who utilize the company's information resources (email, the Internet, etc.) should recognize that its use may be subject to monitoring and/or investigation. Users are expected to cooperate thoroughly while an investigation takes place. Also, users should recognize that when an excessive abuse is detected, he or she may be subject to their local, regional, and/or corporate laws and regulations.

2. Handling of confidential information

(1) Restrict access to confidential information such as corporate business information, personal information of clients, corporate executives, and employees to prevent unauthorized disclosure of sensitive data.

(2) Before providing confidential information to an external company (e.g. business clients, contractors), a non-disclosure agreement which prescribes handling of the information must be in place and the information should be handled propery according to the agreement. When providing confidential information by email or an external storage device, take measures to prevent information leakage by setting a password or using an encrypted device.

(3) In addition to the procedures above, properly manage confidential information, particularly personal information, according to local regional and corporate laws and regulations.

3. Taking IT devices out of the office

(1) Loss or theft of information resources could cause a leak of sensitive data. Removal of these resources from the office should be kept to a minimum. Users should assume full responsibility of devices that have been removed from the office.

(2) To guard against leaking sensitive data, hard disks of PCs taken out of the office should be encrypted. Also, use appropriate safeguards against information loss for other portable devices.

(3) When taking IT devices out of the office, be careful of their loss, theft, and stealthy glance by a third person. Connecting to the external networks should be minimized.

4. Email service use

(1) Only use email services with the company's original domain. Privately-obtained email accounts such as free email services should not be used for business purposes.

(2) Automatic email forwarding is prohibited to prevent disclosure of sensitive data and mail system malfunction except where authorized.

(3) Do not open suspicious messages, URLs, or attachments recieved from unknown senders.

5. Web service use

(1) Non-business access to the Internet consumes business network resources and causes unnecessary exposure to malicious software and viruses. Refrain from accessing the Internet for other than business purpose.

(2) Participation in web-based or email-based surveys, interviews, bulletin boards, or discussion forums in regard to business without the prior approval is strictly prohibited. Even if they express only personal opinions, there is a risk of being interpreted as an official communication or statement of the company.

6. Account/Password

(1) Use only account credentials supplied by system administrators and operate only within the access authority granted to the personnel. A request must be submitted without delay for deletion/change when an account is no longer required due to personnel transfer or when the access authority should be changed.

(2) Accounts supplied for individuals must not be shared with others.

(3) Users should set unguessable passwords, referring to the below:

- Consisting of 6 or more alphanumeric characters
- Combination of upper/lower case letters, numbers, and symbols
- Change at 3 months intervals

(4) Do not divulge passwords or allow them to be visible to others. Change default passwords immediately.

7. Information security education

(1) All executives and employees should take information security education courses periodically to enhance their own security consciousness and to understand the company's and other policies and procedures.

8. When an information security incident occurs

(1) When an information security incident (loss or theft of PC, iPhone, iPad, cellphone, USB memory, information leakage, etc.) occurs, take prompt action to minimize the damage and/or exposure. At the same time, immediately report the incident to the company and Coordinating Office of Autrans Compliance Committee/Information Security Subcommittee.

Ex.) When an IT device is lost/stolen

- Report it to the police and other relevant authority
- Request for the system measures, such as suspending the remote access account and remote wipe
- Report the incident to a supervisor and the Information Systems Department
- Submit the report to the Autrans Compliance Committee/Information Security Subcommittee （Email: it@autrans.com）

Notes to System Administrators

(1) Install servers in an appropriate environment equipped with all necessary power supply, air conditioning, physical security such as locks, etc. A dedicated server room is preferable.

(2) Implement access controls to prevent unauthorized access to IT devices during access to the external network including the Internet.

(3) Adopt appropriate security measures such as anti-virus software and security patches for each IT device.

(4) Allocate redundancy, monitor operation status, and back up important systems to minimize damage to the business in case of a system malfunction.

(5) As a general rule, provide individual user accounts (IDs) and promptly change or delete accounts/IDs resulting from personnel transfers or withdrawal of access authority as appropriate.

(6) Manage privileged IDs (system administrator IDs) separate from general user IDs, strictly limit the users of privileged IDs, and maintain logs, depending on the significance of the systems.

(7) Monitor the status of users' IT usage. When improper usage in violation of this Policy is detected, direct the user to stop such usage.

(8) Establish an emergency contact and a company reporting structure in advance to prepare for information security incidents. Take appropriate action to minimize damage in case of such events (e.g. information leakage).

木田田秀夫