Autrans IT Security Regulations

Article 1 (Basic Policy)
Autrans recognizes IT security as a critical challenge for management, and aim to properly preserve, manage, and utilize valuable IT resources. All those who use, create, and manage the IT resources of Autrans should recognize the importance of IT security and observe these regulations.

Article 2 (Definition of IT Resources)
In these regulations, "IT resources" include all IT devices, external storage devices/ media, information systems, IT environments, and information supplied, lent, or approved by the company. Specially, stored data, various kinds of IT devices (PCs, servers, Smartphones, etc.), external storage devices/media (e.g. USB memory), software, services (email system, the Internet, business application system, etc.), and network environments are included.

Article 3 (Definition of IT Security)
The term "IT security" refers to appropriately utilizing, managing, and protecting IT resources to preserve "confidentiality," "integrity," and "availability."

- The term "confidentiality" refers to securing the system so that only authorized people can access information.
- The term "integrity" refers to securing the system so that data retains its validity, completeness, and accuracy; data 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.

Article 4 (Application Scope/Target)
These regulations apply to all executives and employees (including temporary workers such as temporary staff and subcontracted workers) of the following target companies who handle the IT resources:

- 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 Regulations (e.g., SPC, holding companies)
  - Listed companies and their affiliated companies

A person who uses the IT resources is referred to as "the user" and a person who manages and deploys the IT resources is referred to as "the system administrator."

Article 5 (IT Security Management Organization)
The management organization that maintains IT security of Autrans is named "Autrans Information and IT System Security Committee" (hereafter referred to as "Autrans Compliance Committee").

Article 6 (Responsibility of Managers)

The management of each department is charged with carrying out the following tasks in a responsible manner. Depending on the system, all or some of these tasks can be assigned to auxiliary 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 are followed completely.
2. Securing resources (budget, human resources, etc.) for the execution of security measures.
3. Creating a structure for handing the occurrence of security incidents.
4. Carrying out system risk management activities for the information system 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 "confidentiality," "integrity," and "availability", taking the importance of each factor into account. Upon doing so, ensure that appropriate IT security measures have been implemented to counter such risks.
   (2) Respond to specific system risks as requested by Sojitz Corporation and report the implementation status to the Autrans Compliance Committee.
   (3) If an incident occurs that compromises any of "confidentiality," "integrity," and "availability", immediately take appropriate measures to minimize damage to the system and inform the Autrans Compliance Committee of the incident according to the "Standards for Reporting IT Security Incidents".
5. For confidential information that has been stipulated as such by the IT Security Regulations, fully understand and adhere to the "Sojitz Group's Operating Guidelines for Information Requiring Specified Administrations" to manage information within this category that requires more stringent management.

Article 7 (Precautions for Users)

1. Use of company IT resources
   (1) IT resources of the company are supplied to its employees for business purposes. Use of IT resources of the company for other than business purpose is prohibited unless specifically authorized.
   (2) Only IT resources supplied or approved by the company are permitted. Do not connect unauthorized IT devices to the company's internal 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 it should be necessary to store data on a PC, appropriate measures to safeguard it such as backing up the data must be taken.
   (7) When using external storage devices/media, take measures against information leakage such as using encrypted devices or password-protection of data files. Exporting data from the company's network to external storage devices/media, other than those borrowed from company, is prohibited.

(8) When disposing of IT 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 IT 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 properly 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) Confidential information that requires more stringent management will be designated as information requiring special management that adheres to the "Sojitz Group's Operating Guidelines for Information Requiring Specified Administrations".
(4) 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 IT 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 prevent information leakage, encrypt the entire hard drive on PCs. For computers that cannot be encrypted for technical reasons, such as those with restrictions on applications, do not remove these PCs from the office or save important information on them. Strictly manage these PCs, including implementing measures against loss and theft. Additionally, if IT devices other than PCs are taken outside the office, follow the appropriate information leakage prevention measures.
(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 (a personal email address) should not be used for business purposes. However, the use of a personal email address may be permitted in the following exceptional cases, provided that the required security measures are implemented.
- Exceptional cases:
  - Cases in which a social media site requires official business accounts to be connected to an individual user's personal account

(Example: Official business accounts on Facebook are required to be an individual user's personal account. However, Facebook's Terms of Service require users to "provide for [their] account the same name that [they] use in everyday life" and "create only one account." Therefore, if an employee who already has a personal Facebook account creates a new Facebook account under their name using their company-issued email address, this action would constitute a violation of Facebook's Terms of Service.

- Required security measures:
  - Obtain the account owner's consent to use their personal account.
  - Implement security measures such as multi-factor authentication, two-factor authentication, biometric authentication.
  - Manage and update/remove connected personal accounts as necessary, for example, in the event of employee transfer, resignation, or retirement.

(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 received 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/Passwords

(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) Passwords must be at least 8 characters in length and contain characters from three of the following four types.
  - English upper case characters (A～Z)
  - English lower case characters (A～Z)
  - Numerical digits (0-9)
  - Special characters (! $ # % etc.)

(4) Do not set passwords that can be easily guessed. (Ex. Password1!)

(5) Change passwords immediately if prompted by the system administrator.

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

(7) Do not use the same password that you use for another external service.

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

8. When an IT security incident occurs
   (1) When an IT security incident (loss or theft of PC, Smartphone, Tablet PC, Cell phone, 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 the Autrans Compliance Committee.
   Ex.) When an IT device is lost/ stolen
   - Report it to the police or 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 IT section
   - Submit a report to the Autrans Compliance Committee (Email: it@autrans.com)

Article 8 (Precautions for System Administrator)

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 when connecting to external networks including the Internet. Maintain a log that records internet access usage.
3. Adopt appropriate security measures such as anti-virus software and security patches for each IT device.
4. Do not connect unauthorized IT resources to the company's internal network. Companies that hold information requiring specialized management should set up restrictions to ensure that unauthorized IT devices cannot be connected to the company's internal network.
5. Exporting data from the company's network to external storage devices' media, other than those borrowed from company, is prohibited. Companies that hold information requiring specialized management should set up restrictions to ensure that data cannot be exported from the company's internal network to unauthorized external storage devices/media.
6. Allocate redundancy, monitor operation status, and back up important systems to minimize damage to the business in case of a system malfunction.
7. To prevent information leakage, encrypt the entire hard drive on PCs. For computers that cannot have the hard drive encrypted for technical reasons, such as those with restrictions on applications, do not remove these PCs from the office or save important information on them. Strictly manage these PCs, including implementing measures against loss and theft.
8. As a general regulation, provide individual user accounts (IDs) and promptly change or delete accounts/IDs resulting from personnel transfers or withdrawal of access authority as appropriate.
9. Do not provide PC system administrator authorities to general users.
10. 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.

11. Passwords for information systems must comply with the following specification.
    a. Passwords must be at least 8 characters in length and contain characters from three of the following four types.
        - English upper case characters (A～Z)
        - English lower case characters (A～Z)
        - Numerical digits (0-9)
        - Special characters (! $ # % etc.)
    b. If authentication employs the conditions outlined in (a), regular password changes will be optional.
    c. If authentication does not include the conditions outlined in (a), IT system users will be prompted to change their password once every three months. The same password cannot be used consecutively.
    d. Privileged ID passwords must be changed once every three months.
    e. Information system users should be prompted to change their password immediately after being issued a temporary password.
    f. Set a limit for invalid password attempts. Limit repeated login attempts by locking out the user ID after a certain number of a failed login attempts.
    g. If employing multi-factor authentication, two-factor authentication, or biometric authentication that conflicts with the aforementioned conditions, consult with the Autrans Compliance Committee and decide each case on an individual basis.
12. Monitor usage of IT resources. If inappropriate usage is found, provide guidance to the user on how to correct the behavior.
13. In order to minimize damages in the event of an IT security incident that compromises either "confidentiality," "integrity," or "availability," establish and emergency contact system in advance and make use of management systems supplied by external vendors as necessary.

Established on May 1st, 2024