Information Security Management Regulations
Secretariat of Consortium for analysis and remediation of per- and poly-fluoroalkyl substances

Campus Create Co., Ltd.
Established: March 11, 2025
Effective: April 1, 2025

Chapter 1: General Provisions

Article 1 (Purpose)
These regulations aim to ensure the appropriate protection of information assets provided by consortium member companies, individuals, invited researchers, and business partners (hereinafter "Clients, etc.") from various threats during operations conducted by Campus Create Co., Ltd. (hereinafter "the Company") as the Secretariat of the Consortium for analysis and remediation of per- and poly-fluoroalkyl substances (hereinafter "the operations"). This is to facilitate the smooth and proper execution of the operations.

Article 2 (Definitions)
The definitions of terms used in these regulations are as follows:

Information Assets refer to all items necessary for the proper operation, management, and utilization of information and information systems. This includes hardware, software, networks, recording media, and information, knowledge, and know-how acquired during business activities.

Information Security means ensuring and maintaining the confidentiality, integrity, and availability of information assets.

Confidentiality refers to making information assets accessible only to those with authorized access and protecting them from unauthorized access.

Integrity refers to maintaining consistency and accuracy of information assets by preventing unauthorized alteration or tampering.

Availability refers to ensuring that authorized users can access information assets when necessary, without interruption.

Article 3 (Scope of Application)

These regulations apply to all information assets handled during the operations. In cases where specific operational rules or procedures are defined by contract for the handling of such information assets, those contractual rules shall take precedence.

Chapter 2: Structure of the Information Security Management Regulations

Article 4 (Structure of the Regulations)

These regulations, together with the separately defined "Information Security Management Standards," constitute the Information Security Management Regulations. Matters not covered by these regulations shall be governed by the provisions of the Information Security Management Standards.

Chapter 3: Organizational Structure

Article 5 (Information Security Management Committee)

The Company shall establish an Information Security Management Committee as a supervisory body for information security matters related to the Consortium Secretariat.

The Committee shall promote the implementation of the Information Security Management Standards and provide guidelines for decision-making on information security matters not explicitly covered therein, overseeing all aspects of information security related to the operations.

The Chair of the Committee shall be the President and CEO of Campus Create Co., Ltd.

The Committee shall consist of the Chairperson, committee members appointed by the Chairperson, and the System Administrator.

Article 6 (Committee Members)

Committee Members shall promote thorough implementation of the Information Security Management Standards under the supervision of the Committee.

Article 7 (System Administrator)

The System Administrator shall cooperate with Committee Members to take necessary measures for proper handling of information security in the operations, including awareness-raising and creating a secure environment in accordance with the Standards. The System Administrator may also serve as the Educational Coordinator.

Article 8 (Educational Coordinator)

An Educational Coordinator appointed by the Committee shall plan and implement necessary training to ensure compliance with the Information Security Management Standards when there is a change in personnel assigned to the operations. Training shall be conducted during the handover of tasks or when deemed necessary by the Committee. The Educational Coordinator shall draft the training content, which must be approved by the Committee.

Chapter 5: Risk Assessment and Auditing

Article 9 (Risk Assessment)

The Information Security Management Committee shall continuously assess risks related to information assets from multiple perspectives, taking into consideration technological advances and changes in the business environment. These assessments shall be reflected in the Information Security Management Standards and related measures to ensure the maintenance and improvement of information security.

Article 10 (Audits)

The Auditor shall periodically conduct internal audits to verify compliance with the Information Security Management Standards.

If an audited party receives recommendations or requests for improvement from the System Administrator regarding compliance with the Standards, the audited party must take appropriate corrective actions.

Chapter 6: Sanctions

Article 12 (Actions in Case of Violation of the Standards)

In the event an employee violates the Information Security Management Standards, the Company shall take disciplinary action in accordance with its employment regulations. For second employees, the relevant provisions of the dispatch agreement with the original employer shall apply.

In the event a temporary staff member violates the Standards, the “Part-Time and Temporary Employment Regulations” shall apply.
For contract or dispatched employees from partner companies, the provisions of the respective outsourcing or dispatch contract shall apply.

Supplementary Provision:
These regulations shall come into effect as of April 1, 2025.

Appendix: Information Security Management Standards

Handling of Confidential Information

(Purpose)

These standards outline the procedures for handling (storage, transfer, and disposal) of confidential and personal information provided by Clients, etc., during Operations, to prevent problems before they occur.

(Compliance Requirements)

1.Classification of Information Assets

Information handled in the Operations shall be classified into the following categories:

Class 1 (Public Information): Information for which consent has been obtained to distribute to third parties and make public.

Class 2 (Limited Access Information): Information restricted to member companies and individuals of the Consortium.

Class 3 (Highly Confidential Information): Information that includes personal data or proprietary details meant for internal use only.

Classification shall be confirmed in writing with the information provider.

If information is to be provided to non-members, written consent must be obtained, and necessary agreements must be carried out with relevant parties.

2.Management of Important Information

Class 2 and Class 3 information shall be treated as “important information,” and the following measures shall be applied:

・Labeling

Class 2: The document must explicitly state that it is for limited distribution and identify the authorized audience.

Class 3: The document must clearly state that it contains highly confidential information, restricted from unauthorized access.

・Duplication

Class 3: Duplication requires prior approval from a Committee Member and the Representative. Records of duplication must be kept.

・Distribution

Class 3: Requires approval from the information provider, a Committee Member, and the Representative. Distribution must be logged.

Class 2: Distribution shall be restricted, e.g., by using private cloud sharing links

accessible only to designated parties.

・Encryption

For both Class 2 and Class 3, access to file servers and cloud services must be password-protected. Passwords must be managed securely and updated at reasonable intervals.

・Printing

Class 3: Requires approval from the information provider and the Representative. Records must be maintained.

・Viewing Restrictions

Class 3: Access shall be limited to assigned personnel only.

2. Transfer of Important Information

(1) When sending important information via email, it must be protected with a password.

(2) When sending them via fax, the recipient's number must be carefully verified to prevent mis delivery.

(3) As a rule, external storage devices such as USB memory sticks or SD cards must not be used to carry data outside the company.

(4) When transferring confidential or personal information, services equipped with sufficient security measures must be used.

(5) Before introducing external services such as cloud servers or online storage, the System Administrator shall collaborate with contract staff to conduct a thorough evaluation of the required functions and security measures.

4. Storage Period and Location of Important Information

(1) The storage period for Class 2 information assets is six months from the date of receipt.

(2) For original data such as distributed materials or videos shared exclusively with Consortium members, the storage period is six months from the start date of distribution.

(3) The storage period for Class 3 information assets is also six months from the date of receipt.

(4) Important information must be stored in locations with appropriate access controls to prevent unauthorized access. It must not be taken outside the company or disclosed to third parties without company approval.

4. Measures After Storage Period Ends

Deletion of important information during the storage period is strictly prohibited.

If a contract with a client or partner defines a method for disposing of information, those contract terms shall take precedence.

Paper-based records must be disposed of using methods such as shredding to prevent reuse by third parties.

Outsourcing Management Standards

(Purpose)

These standards aim to prevent potential issues related to the handling of confidential and personal information when entering into outsourcing or subcontracting agreements with external companies, institutions, or individuals.

(Compliance Requirements)

1. The outsourcing or subcontracting partner must meet a sufficient level of information security management, and their credibility and track record must be considered during selection.

2. Contracts must include the following clauses:

(1) Confidentiality obligations

(2) Conditions for data storage and disposal

(3) Procedures for reporting and communication in case of security incidents

(4) Measures including contract termination and compensation in the event of a breach

3. When outsourcing operations involving confidential or personal information, contracts must also include the following:

・Prohibition of information leakage and theft

・Prohibition of processing or copying beyond the agreed scope

・Prohibition of disclosure to third parties

・Conditions for the return, deletion, or disposal of information after contract termination.

PC Handling Standards

(Purpose)

These standards are established to ensure the safety of all PCs managed by the Company and to prevent potential problems in advance.

(Compliance Requirements)

1.Software Installation on PCs

(1) As a general rule, software not required for business operations must not be installed.

(2) Software other than device drivers and official updates must be installed only with approval from the System Administrator.

2. System Maintenance

(1) The OS and installed software must always be kept up-to-date with the latest patches. Unofficial software must not be installed.

(2) If any abnormalities are noticed during PC use, they must be reported immediately to the System Administrator.

3. Usage Restrictions for PCs

(1) Users must log in using their assigned accounts.

(2) Users must not change the assigned PC user without authorization.

(3) Users must use secure passwords and ensure that unlock methods are not disclosed to others.

(4) Any change in PC user must be reported to the System Administrator.

4. Antivirus Measures

(1) Users must strictly follow antivirus protocols.

(2) Users must comply with the items outlined in the “Virus Protection” standards.

5.Disposal of PCs and External Storage Devices

(1) When disposing of PCs or returning leased devices, all data must be completely erased or the devices physically destroyed.

6.Precautions for Taking PCs Outside the Office

(1) Company PCs must not be taken outside the office for non-business purposes.

(2) During travel or in crowded places, PCs must be carried carefully to prevent theft.

(3) When using a PC outside the office, avoid shoulder surfing and use the device in a

secure environment.
(4) PCs must always be kept within reach and not left unattended.
(5) If a PC is lost, immediate action must be taken in accordance with the “Security Incident Reporting and Response” procedures.

Network Usage Standards

(Purpose)
These standards govern the use of networks to ensure confidentiality, protect information assets, and promote effective utilization.

(Compliance Requirements)
1.Connected Devices
Unauthorized devices must not be connected to the internal network.
(2) Precautions for Connecting to Internal Networks
When company-owned PCs are connected to external networks for business reasons, only secure networks must be used.If public Wi-Fi is used, it must be accessed via a VPN or other method approved by the Company.

Email Usage Standards

(Purpose)
These standards are established to ensure the security of information exchanged via email and to prevent related issues before they occur.

(Compliance Requirements)
1.Management of Email Accounts
(1) Email accounts must not be used for non-business purposes.
(2) If an account is suspected to be compromised, it must be reported to the System Administrator immediately.

2. Sending and Receiving Emails
(1) Confidential information such as business-related or personal data must not be sent via email in principle.
(2) If it is absolutely necessary to send such information, encryption, digital signatures, and other measures must be taken as instructed by the Information Security

Committee.
(3) Email addresses must be thoroughly checked before sending messages.
(4) When sending emails to multiple recipients outside the company (e.g., event announcements), recipients' addresses must be hidden to avoid unintended disclosure. Advertising emails must comply with applicable laws.
(5) Passwords used must be difficult to guess and changed regularly.
(6) Suspicious email attachments (e.g., from unknown senders or executable files) must not be opened or executed.

Virus Protection Standards

(Purpose)
These standards are intended to prevent damages such as information leaks or system failures caused by computer viruses.

(Compliance Requirements)
1.Installation of Antivirus Software
(1) As a general rule, antivirus software must be installed on all servers and PCs.
(2) The antivirus software must be selected by the Company and regularly reviewed.

2.Use of Antivirus Software
Users must not alter the settings of antivirus software configured by the System Administrator.

3.Preventive Measures When Using Email and the Internet
(1) Users must not open attachments or click on executable files from suspicious emails, especially those from unknown senders or free email services.
(2) If a suspicious email is received, or a virus is detected, users must report it immediately to the System Administrator.
(3) Users must avoid visiting websites considered unsafe and refrain from downloading files or clicking on unknown URLs.

4.Response to Virus Infections
(1) If infection is suspected, the user must report it to the System Administrator.
(2) For wired LAN connections, the network cable must be unplugged; for wireless connections, Wi-Fi must be disabled.

(3) The System Administrator must take appropriate action in accordance with instructions from the information security department.

Smartphone Handling Standards

(Purpose)

These standards are intended to ensure the safety of all smartphones managed by the Company and prevent potential issues.

(Compliance Requirements)

1.Use of Smartphones

Smartphones used for business must be those provided or loaned by the Company.

2.Usage Restrictions

(1) Users must not change the assigned user without permission.

(2) Secure passwords must be used, and unlocking methods must be kept confidential.

(3) Any user changes must be reported to the System Administrator.

3.Precautions for Taking Smartphones Outside the Office

(1) Smartphones must not be taken out for non-business purposes.

(2) During travel or in crowded areas, devices must be securely carried to prevent theft.

(3) Use in public spaces must be discreet to avoid unauthorized viewing.

(4) Devices must be kept within reach and not left unattended.

(5) If a device is lost, immediate action must be taken in accordance with the “Security Incident Reporting and Response” procedures.

Security Incident Reporting and Response Standards

(Purpose)

These standards ensure appropriate and prompt reporting, response, and recovery in the event of, or suspected occurrence of, a security incident, and establish measures for preventing recurrence.

A security incident refers to any of the following:

(1) Security breaches, e.g., information leaks, virus infections, DoS attacks, loss of media

(2) System or network failures, e.g., hardware damage due to power failure or natural disasters
(3) Threats to information assets, e.g., physical intrusion into buildings

(Compliance Requirements)
1.Preparation During Normal Operations
The Information Security Management Committee must establish and disseminate response procedures in case of incidents.
(1) The Information Security Management Committee shall prepare responses for cases where a security incident occurs or is suspected and ensure thorough dissemination within the company.
(2) The System Administrator shall create detailed response procedures for expected incidents.
(3) Periodic training and reviews shall be conducted to ensure effectiveness and make corrections as needed.
(4) Systems and tools necessary to detect incidents must be in place, ensuring compliance with security standards.

2.Response to Security Incidents
(1) Any individual detecting or suspecting an incident must immediately report it to the Committee and the System Administrator.
(2) The System Administrator, in cooperation with contract personnel, shall determine the cause and scope of damage. If the situation is not covered by pre-established procedures, the Committee shall appoint a responsible officer and form a response team.
(3) Actions must be taken to contain the incident, eliminate the cause, repair affected areas, and restore systems.
(4) If the incident affects clients or business partners, the Committee shall promptly report the facts and prevention measures to them.
(5) Incident-related information must be centrally collected and managed under the officer responsible, including:
・Status and response details
・The impact on stakeholders
・Measures for recurrence prevention
(6) After resolution, the Committee shall work with relevant departments to implement improvements and prevent recurrence.