Attachment: Safety Control Measures

YKK Group companies manage personal information based on the following safety control measures.

Article 1 (Formulation of the Basic Policy)
Establish the basic policy to ensure the proper handling of personal information as an organization.

Article 2 (Development of Regulations on the Handling of Personal Information)
Regulations concerning the specific handling of personal information shall be developed for the prevention of leakage of personal information when handled and for the safe management of personal information.

Article 3 (Systematic Safety Control Measures)

(1) Establishment of an organizational structure
Establish an organizational structure for implementing safety control measures.

(2) Operation in accordance with regulations on the handling of personal information
Personal information shall be handled in accordance with the regulations on the handling of personal information as prepared in advance. In addition, system logs or use records shall be recorded as necessary in order to confirm that the status of operation is in accordance with the established regulations on the handling of personal information.

(3) Establishment of means to confirm the status of handling personal information
Establish means for confirming the status of the handling of personal information.

(4) Development of systems to respond to leaks and other incidents
Cases of leakage, etc. shall be dealt with in accordance with the Notification of Leakage, etc.

(5) Understanding of handling conditions and review of safety control measures
Assess the status of the handling of personal information and implement evaluation, review and improvement of security control measures.

Article 4 (Human Security Control Measures)
Employees shall be thoroughly informed and educated about the proper handling of personal information.

Article 5 (Physical Safety Control Measures)

(1) Management of areas where personal information is handled
Appropriately manage the areas that manage important information systems such as servers and main computers that handle personal information databases and the like related to personal information (hereinafter referred to as "controlled area") and other areas where the clerical work handling personal information is implemented (hereinafter referred to as "handling area").

(2) Prevention of Theft of Equipment and Electronic Media, etc.
Take appropriate measures to prevent the theft or loss of personal information handling equipment, electronic media, documents, etc.

(3) Prevention of Leakage when Carrying Electronic Media, etc.
When carrying electronic media or documents in which personal information is stored (personal information is taken out of a controlled area or handling area or brought into a controlled area or handling area), take secure measures

to prevent the disclosure of personal information.

(4) Removal of Personal Information and Disposal of Devices, Electronic Media, etc.

When personal information is deleted or devices, electronic media, or the like in which personal information is recorded are disposed of, restoration is impossible. When personal information has been deleted, or when equipment, electronic media, etc. in which personal information has been recorded have been disposed of, the record of the deletion or disposal shall be retained. When such work is outsourced, in addition to the supervision based on Article 7, the fact that the outsourcer has deleted or disposed of the work must be confirmed by a certificate, etc.

Article 6 (Technical Safety Control Measures)

(1) Access Control

Appropriate access control shall be implemented in order to limit the scope of the staff and personal information databases.

(2) Identification and Authentication of Accessors

Certify that employees using information systems that handle personal information have legitimate access rights based on authentication.

(3) Prevention of Unauthorized Access from Outside

Introduce mechanisms to protect information systems that handle personal information from unauthorized external access or unauthorized software, and operate them appropriately.

(4) Prevention of Leaks Caused by the Use of Information Systems

Take measures to prevent the leakage of personal information due to the use of information systems and operate them appropriately.

Article 7 (Supervisory Responsibility for the Contractor)

In cases where the handling of personal information is entrusted in whole or in part, the following measures shall be taken to provide the entrusted person with the necessary and appropriate supervision as the entrusted:

1. In selecting a contractor, confirm in advance that the items specified in this Safety Control Measures will be correctly implemented in accordance with the contents of the contract work in order to confirm that the safety management measures of the contractor are equivalent to those of this Safety Control Measures.
2. A contract shall be concluded with the selected contractor and the contract shall include provisions to enable the contractor to rationally grasp the status of entrusted personal information handling by the contractor, as well as the content agreed by both the contractor and the contractor, as necessary and appropriate security control measures for the handling of the personal information.
3. In order to grasp the handling status of entrusted personal information by the subcontractor, an audit shall be conducted periodically to investigate the degree of implementation of the content included in the entrustment contract, and the handling status of entrusted personal information by the subcontractor shall be appropriately monitored by an evaluation, including reviewing the content of the entrustment.
4. Subcontracting by contractors is prohibited.

Article 8 (Measures against Leakage, etc.)

In the unlikely event that personal information is leaked, lost, or altered, the following measures shall be taken.

(1) Internal reporting and prevention of damage expansion

Immediately report the incident to the responsible person and take necessary measures to prevent the damage caused by the leak or other incident from spreading further than when it was discovered.

(2) Investigation of the Facts and Investigation of the Causes

Necessary measures shall be taken to investigate the facts of the leakage case and to investigate the cause.

(3) Identification of the scope of impact

Determine the extent of the impact of the facts identified in (2) above.

(4) Examination and Implementation of Recurrence Prevention Measures

Based on the results of (2) above, we will promptly take necessary measures to review and implement measure to prevent the recurrence of leaks and other incidents.

(5) Communication to the Person Who May be Affected

Depending on the details of the case, from the viewpoint of preventing secondary damage and the occurrence of similar cases, the facts shall be promptly communicated to the person concerned or put in a state where the person can easily know.

(6) Publication of Facts and Measures for Recurrence Prevention

According to the contents of the leaks, from the viewpoint of preventing secondary damage and the occurrence of similar incidents, we will promptly publicize the facts and the recurrence prevention measures .

(7) Notification to the Supervisory Body

Depending on the nature of the leak and if required by laws or regulations applicable to the jurisdiction concerned, we will promptly report to the supervisory body (by the deadline set forth by applicable laws and regulations at the latest).