

Overview of Security Control Measures

1 Design of Basic Rules

We, a member of YKK Group, have designed the YKK Group Privacy Policy and adopted this Policy as our basic policy on personal data protection. In accordance with this Policy, we will comply with applicable laws, regulations, and guidelines to ensure proper handling of personal data. This Policy includes contact information when you have any question or complaint about our processing of your personal data.

2 Creation of Personal Data Handling Rules

We have also laid down the YKK Group Personal Data Control Rules. These Rules includes provisions regarding personal data processing procedures, the person in charge of personal data handling, and the person's job duties and responsibilities when we acquire, use, store, provide, delete, erase or otherwise process personal data.

3 Systematic Security Control Measure

We appoint Information Control Enhancement Manager, who are in overall charge of personal data protection, and Manager of a data handling department. In addition, we have set up cross-sectional Information Security Committee and clearly defined the authority and responsibility regarding personal data protection, and we clearly specify personnel who are assigned the task of processing personal data, and clearly defines the scope of personal data to be handled by such personnel. We have set up an effective system for contacting the Information Security Committee. If we become aware of a fact or sign that someone is in breach of applicable laws or internal rules, we will immediately notify the Committee of such a fact or sign.

We do a daily inspection of the way personal data are handled and regularly conduct an internal auditing of personal data handling in accordance with an internal auditing plan.

4 Personal Security Control Measure

-We clearly define functions and responsibilities for personnel comprising officers, employees, temp workers and others.

-A department manager is responsible for making internal rules regarding personal data processing well known to all of his or her subordinates.

-We give our personnel a periodic training to teach them the important points to keep in mind when they engage in information security (personal data included).

-We receive "Confidentiality Agreement" in writing from personnel when they join us and when they leave us.

5 Physical Security Control Measure

-Within the area where personal data are processed, we control entering and leaving the room and limit equipment that is brought into the room. We have also taken steps to prevent an unauthorized

person from viewing personal data.

-We have taken measures to prevent theft or loss of equipment, electronic media, and documents containing personal data. We have also taken steps to prevent personal data from being easily known or available when such equipment, electronic media, and documents are carried.

6 Technical Security Control Measure

-We restrict personnel who have access to personal data and the scope of personal databases by implementing access control.

-We have adopted measures to protect our personal data processing system from unauthorized access and malicious software.

7 Grasping of External Environment

We use our best effort to identify foreign countries and the location of overseas servers that are handling personal data, and we are taking proper security control measures by grasping personal data protection systems in foreign countries. If you have any question about security control of personal data in an external environment, we will immediately answer your inquiry.