

JaCER Information Security Policy

The Japan Center for Engagement and Remedy on Business and Human Rights (hereinafter "JaCER") recognizes that maintaining and promoting information security in the operation of the Engagement and Remedy Platform and other activities is crucial for ensuring that stakeholders, companies, and other parties can use the Engagement and Remedy Platform with confidence. To this end, JaCER commits to the following measures.

Furthermore, JaCER has established its information security rules to implement this policy and requests that JaCER's officers, employees, partners (hereinafter "JaCER's staff") comply with this policy and the information security rules.

1. **Organizational Safety Management Measures**

JaCER will appoint an Information Security Officer from among the directors. The Information Security Officer, under the supervision of the Board of Directors, will promote information security measures taken by JaCER's staff.

2. **Human Safety Management Measures**

JaCER will require JaCER's staff to comply with necessary measures to ensure information security and will involve them in information security education and training.

3. **Physical Safety Management Measures**

JaCER will implement measures to physically restrict unauthorized access to information by third parties, including the office access control.

4. **Technical Safety Management Measures**

JaCER will undertake technical safety management measures, including account management, access control, and ensuring the security of software and hardware.

5. **Information Lifecycle Management**

JaCER will implement appropriate measures to maintain information security throughout the information lifecycle (receipt/collection, storage, transfer/disclosure, removal/duplication, disposal/return). Additionally, JaCER will conduct regular inspections and audits regarding the implementation status of information lifecycle management.

6. **Response to Security Incidents**

In the event of incidents involving information leakage, loss, or damage (hereinafter "security incidents"), JaCER will take appropriate measures, including detection,

investigation, damage containment, communication with information subjects, and prevention of recurrence.