

Basic BCP Policy

Adopted: March 24, 2006

Revised: January 5, 2009

June 17, 2011

October 11, 2011

June 16, 2014

July 24, 2015

February 12, 2016

March 31, 2021

Japan Securities Depository Center, Inc.

Japan Securities Depository Center, Inc. and JASDEC DVP Clearing Corporation (hereinafter referred to as “JASDEC Group”), in recognition of their role as a critical settlement infrastructure in the capital market and to ensure swift execution of continued operation and recovery in the event of an assumed risk, has defined a Business Continuity Plan (BCP) to ensure the reliability of its operations based on the policies outlined below.

1. Scope of BCP

(1) Assumed Risks

- JASDEC Group presumes three classes of SBD cases: widespread disasters due to a natural disaster, epidemic, or disruption of social infrastructure; isolated disasters due to fire, or terrorist attack; and system failures within the Group.

(2) Scope of Application

- The BCP applies to executive officers and employees of JASDEC Group, temporary staff engaged in work for JASDEC Group, and staff of subcontractors for system development /operations, etc.
- For JASDEC participants and related entities, JASDEC Group seeks an understanding of the BCP on a routine basis and puts in place the systems to ensure contact with them in the normal course of their activities.

(3) Priority Functions to be Continued or Recovered

- JASDEC Group will prioritize the continuity or restoration of Critical Functions (CF) that involve contact with JASDEC participants and related entities, as well as business functions regarding security settlements and corporate actions.

2. Recovery Time Objective

The recovery time objective (the target time from the initial cessation of a business function to its restoration) in the event of a SBD is defined generally as being within two hours, with recovery of CF to be achieved within this timeframe. JASDEC Group will also aim to complete in-progress settlements within the day.

3. Action Policy

In the event of a SBD, JASDEC Group will continue to conduct business as far as possible, or resume business operations as soon as possible, in order to minimize the effect on JASDEC participants and related entities.

(1) Widespread Disasters

- Widespread disasters are presumed to affect JASDEC participants and related entities as well as JASDEC Group as a whole, and result in disruption of social infrastructure such as electric power supply, communications, and transportation.
- In the event of a widespread disaster, the following actions will be taken in principle:
 - 1) Establishment of a BCP Countermeasure Office
 - 2) Collection of information and assessment of the situation
 - 3) Decision on appropriate measures
 - 4) Ensuring contact with JASDEC participants and related entities
 - 5) Activation of Alternative Operations (continuation of operations at an alternate office)
 - 6) Recovery Preparations
- In the event that JASDEC Group main office is deemed inoperable due to a widespread disaster, JASDEC Group will continue to operate and respond to outside inquiries at its alternate office.

(2) Isolated Disasters

- Isolated disasters are presumed to affect JASDEC Group only, with JASDEC participants and related entities capable of normal business functions.
- In the event of an isolated disaster, JASDEC Group will take measures as outlined above in "(1) Widespread Disasters", and work to resume business operations as soon as possible, taking into consideration the fact that JASDEC participants and related entities continue to conduct operations as normal.

(3) System Failures in JASDEC Group

- System failures are presumed to result in the inaccessibility of all or part of JASDEC Group's computer systems.
- JASDEC Group will respond to system failures according to the principles outlined

separately in the Basic Policy on Response to System Failure.

- In the event of a system failure, where a BCP Countermeasure Office is established, JASDEC Group will follow the course of action outlined above in "(1) Widespread Disasters".

4. Establishment of Framework for Emergency Action

(1) Establishment of BCP Countermeasure Office

- In the event of a SBD deemed as having the potential to impede business functions, JASDEC Group will establish a BCP Countermeasure Office in charge of assessing damage, ensuring contact with JASDEC participants and related entities, and making decisions regarding the continuity of business operations.

(2) Securing Necessary Personnel

- In the event of a SBD, JASDEC Group will secure the necessary personnel to implement the BCP with giving top priority to the safety of its executive officers and employees, temporary staff engaged in work for the Group, and staff of subcontractors for system development/operations, etc. as soon as possible.
- JASDEC Group will utilize telecommuting to secure personnel.
- To ensure the continuity of CF in the event of a widespread or isolated disaster, the Group will assign necessary personnel to its alternate office during periods of normal operation.

(3) Securing Lines of Communication

- In order to secure necessary personnel in the event of a SBD, JASDEC Group will put in place a system to ascertain the safety status of personnel through a Safety Confirmation System, etc.
- To secure communication in the event of a SBD, JASDEC Group will put in place a system to utilize a number of communications options including an emergency telephone priority service, JASDEC TARGET website, and message centers on the Group website, in addition to telephone, fax and e-mail.

(4) Alternate Office

- JASDEC Group has established an Osaka office to continue operations, provide information on the status of its operations, and respond to inquiries from outside even in the event that the Group main office becomes inoperable or inaccessible due to the disruption of social infrastructure such as electric power supply, communications, and transportation.

(5) Reinforcement of IT Systems

- JASDEC Group IT systems are based on a redundant configuration and installed in a robust data center (main system center). In addition, JASDEC Group maintains a remote backup system in a robust data center (backup center). In the event that the main system center becomes inoperable or suffers a system failure and cannot resume normal functions within a short period of time, the group will promptly switch operations to the backup system.

The main system center and backup center are connected via high-speed dedicated communication lines, with main system center data reflected in the backup center in near real-time.

(6) Simulation Exercises

- JASDEC Group will conduct periodic verifications of procedures regarding its safety confirmation, BCP Countermeasure Office establishment, and switching to alternate office.
- JASDEC Group will conduct test exercises switching to the backup system at least once annually.