Basic Policy on Cybersecurity

Adopted April 1, 2026

JASDEC Group (comprising Japan Securities Depository Center, Inc. and JASDEC DVP Clearing Corporation) recognizes more strongly than ever that, as a critical settlement infrastructure supporting the capital markets, interruption of operations caused by cyberattacks constitutes a significant risk that could have a serious impact on confidence in the financial system. In light of this, JASDEC Group has established a “Basic Policy on Cybersecurity” as the fundamental policy for cybersecurity management in order to ensure cybersecurity necessary for the stable and appropriate provision of services.

1. Initiatives to ensure cybersecurity

JASDEC Group positions cybersecurity as one of the important management issues. Under the leadership of senior management, JASDEC Group will foster a cybersecurity-conscious organizational culture that emphasizes cybersecurity and promote group-wide initiatives taking into account the potential impact and risks that cyberattacks may pose to operations.

2. Establishment of a cybersecurity management structure

JASDEC Group will ensure appropriate governance that enables appropriate management decision-making by appointing a Cybersecurity Executive responsible for overseeing cybersecurity across JASDEC Group and establishing communication channels with the Board of Directors and senior management.

Taking into account evolving cyber threats, requirements from relevant stakeholders, and internal and external environments including laws and regulations, JASDEC Group will establish and operate a Cybersecurity Management Structure led by the Cybersecurity Executive and will continuously improve the structure.

3. Thorough implementation of cybersecurity measures

JASDEC Group will implement initiatives based on the concept of “security by design,” which incorporates security requirements from the planning and design stages of services and systems, and will take a thorough measures to prevent unauthorized access to, leakage, tampering, loss, destruction and/or usage disruption of information assets caused by cyberattacks. Furthermore, JASDEC Group will collect, analyze, and evaluate cyber threat intelligence and vulnerability information, and will continuously improve the measures implemented.

4. Strengthening third-party risk management

To prevent interruption of operations caused by cyberattacks originating from the supply chain, JASDEC Group will identify its third parties and related operational processes across the supply chain in connection with the operation of systems and services. After assessing risks arising from third parties, JASDEC Group will establish an appropriate third-party risk management structure and conduct continuous monitoring throughout the lifecycle.

5. Securing and developing cybersecurity human resources
JASDEC Group will ensure cybersecurity across the organization by securing and assigning personnel with specialized expertise to departments responsible for cybersecurity and providing comprehensive cybersecurity education and training to directors, officers, employees, and other relevant parties engaged in the Group's operations.