Calbee Group Information Security Policy

・Basic Philosophy

For the Calbee Group, the use of digital technologies and IT is a key means of driving transformation. At the same time, maintaining information security is essential to their continued safe and secure use. We therefore regard information assets as a fourth category of assets, alongside people, physical assets, and financial resources, and take appropriate measures to protect them from cyberattacks and other threats, including unauthorized access, disclosure, modification, or loss, as well as disasters. Furthermore, to ensure business continuity and maintain public trust, we take a Group-wide approach to information security in accordance with the following policy.

・Scope

This Policy applies to Calbee, Inc. and all of its subsidiaries worldwide (collectively, the “Group”).

・Information Security Policy

1.Management Responsibility

The Group’s senior management recognizes information security as a management-level issue and will ensure that the necessary organizational structures, personnel, and budget are in place, while promoting Group-wide, ongoing information security efforts.

2. Compliance with Laws, Regulations, and Contractual Requirements

The Group will comply with laws, regulations, and guidelines related to information security in each country and region, as well as contractual obligations to customers and business partners. To that end, each Group company will establish and implement rules and procedures in accordance with this Policy.

3. Organizational Structure

The Group will establish an organizational structure with clearly defined roles and responsibilities related to information security and will work to strengthen governance across the entire Group. In establishing this structure, the Group will consider how it aligns with other risk management structures, such as those for internal control and privacy protection.

4. Protection of Information Assets and Secure Use of Digital Technologies and IT

The Group will treat the information and systems needed to support its business activities as the information assets and manage them accordingly. It will also establish an environment to enable the safe and appropriate use of digital technologies and IT. As part of this effort, the Group will identify the assets to be protected, assess the associated risks, and plan measures to address those risks. The Group will also require business and IT partners that handle information assets to ensure their appropriate protection and secure use.

5. Education and Awareness

The Group will provide education and training to all employees who handle information assets, regardless of employment status, to enhance their knowledge, awareness, and response capabilities regarding information security.

6. Incident Prevention and Response

The Group will establish mechanisms to prevent security incidents and will review and update them in response to changes in its business environment and threat landscape. In the event that an incident should occur, the Group will respond promptly and appropriately, and will seek to minimize its impact, investigate the cause, and prevent recurrence.

7. Review, Audit, and Continuous Improvement of Initiatives

The Group will conduct periodic reviews, assessments, and audits to evaluate the effectiveness of its information security measures and will make continuous improvements based on the results. In addition, the Group will actively monitor external developments in order to make improvements in line with advances in information technology.

8. Protection of Personal Information

The Group will manage personal information appropriately and in accordance with the applicable laws and regulations of each country and region and the Group's Privacy Policy.

Effective Date: October 8, 2026