Business Engineering Corporation
KDDI Otemachi Bldg., 1-8-1, Otemachi, Chiyoda-ku, Tokyo 100-0004, Japan

B-EN-G

White paper on GLASIAOUS and GLASIAOUS+

Summary

This document describes the security management of various cloud services provided by Business Engineering Corporation (hereinafter referred to as "B-EN-G") as of March 2025, based on the Company's cloud service information security policy.

Overview of the cloud services

Services

Cloud-based accounting & ERP services that support business growth

Location and jurisdiction of the cloud services

B-EN-G is a Japanese corporation with its head office in Tokyo, Japan. Its cloud services are developed and operated mainly in Japan. In addition, the data on the cloud may be stored in the overseas server area using third-party cloud services such as Microsoft Azure.

Cloud data storage	Countries where cloud data is stored
Microsoft Azure	Japan, Southeast Asia, East Asia, USA, Western Europe, etc.

Compliance with Contracts in Cloud Service Usage

Our organization complies with the contractual terms agreed upon with the IaaS providers (cloud service providers) we use.

Additionally, we adhere to the contractual agreements established with our cloud service customers.

Development and operation structure of the cloud services

B-EN-G makes and enters into nondisclosure agreements with all our employees involved in development and operation, which include articles that they shall not use confidential information for their private purposes or disclose it to outside. In addition, B-EN-G conducts information security training for our employees on a regular basis.

Outsourcing of development and testing operations, and information security management of contractors

B-EN-G outsources part of its system development and testing tasks to partner companies both domestically and internationally. A confidentiality agreement is signed

with these contractors, and in addition, information security requirements are established and mutually agreed at the time of contract.

Backup methods of the cloud services and provision of backup data

B-EN-G maintains data backups for its entire service in case of a cloud service failure. Backups are relocated to and stored in another region, and in the event of a service failure, B-EN-G is prepared to quickly recover the service from the backups.

Frequency of backups	Remote storage
Daily	Provided

Time of reference for the cloud services

For the integrity of data on the cloud services, B-EN-G ensures the accuracy of time stamps of information registration, update, deletion, and various logs by synchronizing with the following time server.

Synchronization Destination
Microsoft Time Server

Encryption of the cloud services

As a countermeasure against data leakage or removal due to internal fraud, B-EN-G encrypts the communication path and data on the cloud services.

Target	Encryption
Password	Yes
Communication with the system	Yes
Backup data	Yes

Other security features for the cloud services

We provide the following security features to customers for data in the cloud services. Connection source restrictions based on IP addresses are provided as an optional feature. With authentication integration provided as an optional feature, it is possible to use multi-factor authentication (MFA) from the integrated system. Similarly, single sign-on (SSO) from the integrated system can also be used.

Security features	Basic/Option
IP address restriction function	Provided as an optional feature
Multi-factor authentication	Supported by the MFA function of the authentication integration provided as an optional feature
SSO (Single Sign-On) function	Supported by the SSO function of the authentication integration provided as an optional feature

Detection of cybersecurity attacks

AS to the cloud services, B-EN-G has prepared for the rapid detection and treatment of abnormalities by introducing a real-time detection mechanism for the following targets, as well as carrying out vulnerability diagnosis on a regular basis.

Target	Detection
Virus	Available
Failure	Available
Attack	Available

Information security incident reporting targets and notification methods

In the case B-EN-G determines that a specific customer has been affected by an information security incident, B-EN-G will notify the representative registered as contact address. In addition, in the event of an incident that broadly affects customers, such as a service outage, B-EN-G will notify the customers on the top page of its service website.

Report content	Notification method
Service failure	Email, Service website

Preparing a cloud service disaster response plan

B-EN-G makes commercially reasonable efforts to ensure that the cloud services' operating rate is 99.5% or higher per year as SLA.

Handling of personal information in the cloud services

Customer’s operational data stored in the cloud services may contain personal information. As a general rule, this personal information is managed by the customer.

B-EN-G handles customer’s data containing personal information to provide the cloud services. The operations and purposes for which such data is handled are limited to the following:

・Service environment setup (initial setup, granting of administrator accounts)
・Obtaining backup data for the service environment
・Recovery from backups
・Verification tasks using customer’s data in the event of a system failure

Provision of cloud operational data containing customer’s personal information to third parties

The following are cases where operational data containing customer's personal information is provided to third parties other than B-EN-G.

Cases provided to third parties	Recipient	Purpose
Verification tasks using customer's actual data in the event of a system failure	Development/verification contractor	System operation verification only
In the event of a legally binding request from law enforcement agencies	Law enforcement agencies	Purpose of law enforcement agencies

ver.1.0 October 1, 2023 (First Edition)

ver.1.1 October 1, 2024 (Revised)

ver.1.2 March 31, 2025 (Revised)