BlueYonder
Cybersecurity

Customer Security Measures

Version 2.0
Effective: April 14, 2023

Blue Yonder has implemented and will maintain the following security measures and controls that leverage National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), specifically ISO 27001, ISO 27701, System and Organization Controls (SOC), both SOC 1 Type II and SOC 2 Type II series of control standards as its baseline to protect Customer Data and ensure the ongoing confidentiality, integrity and availability of Blue Yonder's products.

Measure	Description
Due Diligence	• Blue Yonder's security practices and standards are designed to safeguard Blue Yonder's corporate environment and to address business objectives across information security, system and asset management, development, and governance. • Regional and regulatory requirements are consistently monitored and are fundamental topics of Blue Yonder's awareness, training, and educational efforts. • Blue Yonder maintains an appropriate data privacy and information security program, including policies, standards and procedures for physical and logical access restrictions, data classification, access rights, credentialing programs, record retention, data privacy, information security and the treatment of personal data throughout its lifecycle. • Cybersecurity and Data Privacy policies are reviewed annually.
Organizational Security	• It is the responsibility of all Blue Yonder Personnel and contractors who are involved in the processing of Customer Data to comply with our practices and standards. Blue Yonder's Chief Security Officer is responsible for the following activities: ○ **Security Ownership**. Blue Yonder's information security program establishes and maintains a formal hierarchy of security professionals led by the Chief Security Officer who is responsible for coordinating and monitoring security policies and procedures. ○ **Security Roles and Responsibilities.** Blue Yonder Personnel and contractors sign a Confidentiality agreement and Acceptable Use Policy on hire. ○ **Risk Management.** Blue Yonder follows a risk-based approach for risk management in order to categorize systems, select and implement appropriate controls based on risk, assess, and verify the functional implementation of controls, explicitly authorize a system's deployment, and continuously monitor the system for weaknesses and compliance. Blue Yonder ensures vulnerability assessment, patch management, and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.

Measure	Description
	○ Blue Yonder conducts vulnerability scanning and patching in accordance with documented frequencies defined in established policies and procedures.
Awareness and Training	• Blue Yonder ensures that Personnel and contractors complete information security and data privacy awareness trainings and are made aware of their responsibilities with regards to information security as well as data privacy and the handling of Customer Data at least one time per year. • Blue Yonder provides Personnel with clear instructions and awareness for using Customer Data and Information Technology (IT) systems, including but not limited to, the following requirements: ○ Keep Confidential Information and IT equipment secure at all times, including when travelling or working out of the office or from home. ○ Keep UserIDs, passwords and PINs for IT systems and devices, confidential and protect them from unauthorized access. ○ Do not connect untrusted removable media devices to IT systems or laptops. ○ Keep devices used to access Customer Data and IT systems up to date with security updates. ○ Handle Customer Data in accordance with Blue Yonder's classification and documented handling procedures. ○ Only share Customer Data with authorized individuals on a need-to-know basis. ○ Encrypt Customer Data when emailing or sharing externally. ○ Check before sending emails containing Customer Data and that all the recipients are authorized to receive the Customer Data. ○ Be aware of phishing and do not click on links in emails or documents or provide any Customer Data over the phone without verifying the caller. ○ Do not use personal instant messaging services or personal email accounts to conduct Customer business or to share or receive Customer Data. ○ Be discreet when discussing Customer Data so you cannot be overheard and do not share Customer Data online, including using the social media, external social networks, instant messaging or blogging sites. ○ Maintain a clear desk and a clear screen so that Customer Data cannot be viewed or accessed by unauthorized individuals. ○ Do not leave Customer Data unattended or on voicemails.

Measure	Description
	○ Securely dispose of paper and other media using correct procedures. ○ Report security events and non-compliance to security policies promptly and without delay.
Asset Management	• Blue Yonder's practice is to inventory all media where its data is stored, track and manage those information system assets and allow only authorized access. • Blue Yonder ensures the segregation of production environments and data from the development, test, and sandbox environments. • Blue Yonder maintains an Information Classification Policy, Information Handling and Labeling Standards, which are reviewed on an annual basis. • Access to Customer Data is appropriately restricted.
Physical Access	• Ensuring physical security of locations in which Customer Data is processed by doing the following: ○ **Physical Access to Facilities**. Blue Yonder limits access to authorized personnel at premises, buildings, or rooms where Customer Data processing systems are located. ○ Blue Yonder ensures a high level of physical security in data centers including multiple layers of access controls, detection, and monitoring controls. ○ Blue Yonder customer support offices are secured with controlled visitor access, monitoring, guarding and key card access. ○ Blue Yonder premises maintain a safe level of fire and environmental protection in accordance with local laws. ○ **Physical Access to Components**. Blue Yonder requires visitors to its data centers to sign a visitor's log and visitors are escorted by Blue Yonder Personnel. ○ **Protection from Disruptions.** Blue Yonder uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference. ○ **Appropriate Disposal**. Blue Yonder on request will securely delete Customer Data in accordance with current industry standards such as NIST 800-88 or an equivalent.
Communications and Operations Management	**Operational Policy.** Blue Yonder maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data.

Measure	Description
	Security Operations. Blue Yonder manages support of implemented security solutions, monitors, and scans Blue Yonder's information technology environments, and its assets. - Blue Yonder has a dedicated team of Business Continuity Management professionals. - Changes to operating environments are logged, monitored, and reviewed. The organization utilizes separate data center locations and leverages a centralized Security Information and Event Management (SIEM) solution to aggregate and correlate logs (from system files, security files, etc.) for greater insight into the security of the environment. Through 24x7 threat detection capability, logs are continuously monitored. - Blue Yonder ensures appropriate geographical redundancy is in place. - Blue Yonder's data is stored redundantly in multi-geo global public and private cloud environments.
Access Control	**Access Policy.** Access to Blue Yonder's systems is restricted to authorized users. Formal procedures and controls govern how access is granted to authorized individuals and the level of access that is required and appropriate for that individual to perform their job duties. - New access to network, systems, and data are approved and documented. - Blue Yonder Users are prohibited from sharing accounts. - Blue Yonder employs the principle of least privilege throughout all accounts and access to prevent any account from having unnecessary access. - Blue Yonder employs the principle of Separation of Duties throughout all accounts and access to prevent any account from having too much access. - Blue Yonder reviews the access requirements and permissions of accounts regularly. - Blue Yonder utilizes Multi Factor Authentication (MFA) for remote User virtual private network access to systems containing Customer Data. - Blue Yonder enforces the use of password complexity, minimum length of eight (8) characters, password changes every 60 days, and lockout after five (5) unsuccessful login attempts. - Blue Yonder reviews privileged account access to relevant Customer Data quarterly and monitors account access for unusual sign-in attempts. - Blue Yonder has implemented identity and access management processes to control access and authenticate Users prior to granting access. - Blue Yonder revokes access immediately for Users no longer working on the Services or those that no longer require access.
Security Incidents and Response Plan	- Blue Yonder has various technical controls suitable for detecting potential incidents on networks, endpoints, and applications.

Measure	Description
	• Blue Yonder has a documented Security Incident Response Plan based on NIST standards. • Blue Yonder centralizes multiple data sources for the purpose of log correlation and rapid response. • Blue Yonder ensures its incident response capacity includes legally admissible forensic data collection and analysis techniques. • Blue Yonder ensures physical and logical access to production environments is logged and monitored with alerting configured for anomalous events. • Blue Yonder maintains security incident response plans to manage response to security events, and they are tested on at least an annual basis. • Blue Yonder will report confirmed breaches of Customer Data or the environment under which it is stored (to the extent the same is under Supplier's direct control) to Customer within 48 hours from the time Blue Yonder confirmed the breach of Customer Data. • Blue Yonder assesses security events and suspected incidents against defined criteria and responds to incidents in such a way that takes into consideration their potential impact to the Customer and the Customer's Affiliates. • Blue Yonder will consult with the Customer prior to conducting forensic investigation following an incident affecting Customer Data or the environment under which it is stored (to the extent the same is under Supplier's direct control) and conduct investigations in accordance with legal requirements for preserving evidence. Blue Yonder will keep Customer apprised of the forensic investigations and remediation. • Blue Yonder will contain and mitigate incidents in accordance with documented incident management procedures and response plans. • Blue Yonder will mitigate newly identified vulnerabilities. Any vulnerabilities that cannot be mitigated, that could have a material impact on the security of Customer Data will be reported to the Customer. • Blue Yonder will conduct post incident reviews to identify root-causes and identify actions required to minimize the risk of similar incidents re-occurring. Response strategies and plans will be updated in response to any lessons learned.
Data Transmission Control and Encryption	• Blue Yonder will make available the following types of data transfers: ○ (i) a Secure FTP ○ (ii) an AS2 Communications Channel

Measure	Description
	○ (iii) APIs via secure protocols or via a secure channel (when such APIs are supported) for transfer of data between the Customer and Blue Yonder. ○ Unless otherwise indicated, the Customer will initiate the pushing of input data from their end to Blue Yonder and the pulling of data from Blue Yonder to the Customer. ○ One end point is included to connect to the Production Environment. A further end point is included and shared across the development and test environments. If needed, additional end points are available for additional fees. • Blue Yonder encrypts Customer Data in transit. • Customer Data is transferred in transit via HTTPS, SFTP or AS2 using TLS 1.2 or higher. • Customer Data at rest is encrypted using AES256 bit encryption at the disk array. • Blue Yonder maintains an established Cryptography Policy aligned with current best practices. • Blue Yonder prohibits the use of deprecated ciphers and requires the use of strong public keys and algorithms.
Secure Operation of Information Systems	• Blue Yonder maintains a documented change management process with appropriate escalations and approvals for emergency and production availability issues. • Blue Yonder enforces Mobile Device Management on cellphones, smartphones, tablets, laptops, and desktop computers. • Blue Yonder utilizes an advanced endpoint detection and response platform.
Availability Control	• Blue Yonder business continuity and disaster recovery plans are consistent with industry standard practices. Recovery planning support our documented risk management guidelines and is reviewed annually. Blue Yonder ensures each customer environment is logically segmented and isolated from other customer environments via network controls such as firewalls, web application firewalls, intrusion prevention and detection, and network access control points. • Blue Yonder designs and periodically reviews network architecture in accordance with layered defenses, or a Defense-in-Depth approach. • A 24-hour on-call procedure has been implemented to provide support for production systems. • Monitoring software on production servers and applications automatically alerts Personnel of error conditions.

Measure	Description
	• Commercial anti-virus software is installed on production servers to mitigate the risk of virus threats. • Production Windows servers are set to automatically update virus definition files.
Data Security	• Blue Yonder has a formal, documented, well-practiced third-party risk management program and ensures through a repeatable process that its third parties have similar security controls and data security requirements as exemplified by Blue Yonder itself, in effect making them secure extensions of Blue Yonder suitable for the processing and storage of Customer Data. • Blue Yonder maintains procedures and controls to protect the security of Customer Data (to the extent such Customer Data or the environment under which it is stored is under Supplier's direct control) at every stage of its lifecycle from creation through processing, storage, and disposal. • Blue Yonder enforces full-disk encryption on portable devices accessing Customer Data. • Blue Yonder maintains the security of systems and User laptops using standardized builds that include a hardened operating system, malware protection, and host-based security software. Only Blue Yonder owned and managed laptops are allowed to connect to Blue Yonder's network and systems. • Configuration changes are limited to authorized individuals, in accordance with documented change management procedures and using approved systems and tools. • If Customer Data is stored on removable media, it is hardware encrypted and protected by a password. • Blue Yonder will not use Customer Data for testing without the prior consent of the Customer.
System Development and Maintenance	• Blue Yonder necessitates appropriate levels of segregated management approvals and security validations throughout the process before allowing production changes to code that would impact Customers. • Blue Yonder obtains security design approval through each step of the development process and before each production release. • Blue Yonder applications and SaaS infrastructure are provisioned, designed, architected, implemented, and monitored continuously in accordance with industry standard security best practices. • Blue Yonder deploys security controls in accordance with policies that prescribe a high degree of restriction and monitoring to protect Customer Data.
Security and Privacy	• Blue Yonder ensures its security controls are appropriate to adhere to, but protect the information's confidentiality, integrity, and availability.

Measure	Description
	• Blue Yonder may allow specific geographical data storage locations as deemed appropriate in accordance with legal and regulatory requirements. • Blue Yonder upon request, facilitates a formal process for providing copies of, or ensuring the deletion of, Customer Data in accordance with legal and regulatory requirements. • Blue Yonder is committed to transparency concerning Customer Data disclosure requests in accordance with its PII disclosure request procedure. Blue Yonder will decide together with qualified external or internal legal counsel at Blue Yonder's discretion whether such requests should be approved or rejected. In case of a Customer Data disclosure request from a third-party Blue Yonder consults with the Customer as part of the decision-making process unless there is a legal obligation to maintain confidentiality of the legal request. Legally binding requests which are submitted by an appropriate authority must be complied with. Otherwise, unless prohibited by the applicable law, Customer is making the decision whether to allow the request. Blue Yonder publishes an annual report concerning Customer Data disclosure requests received. The Transparency Report is located here.