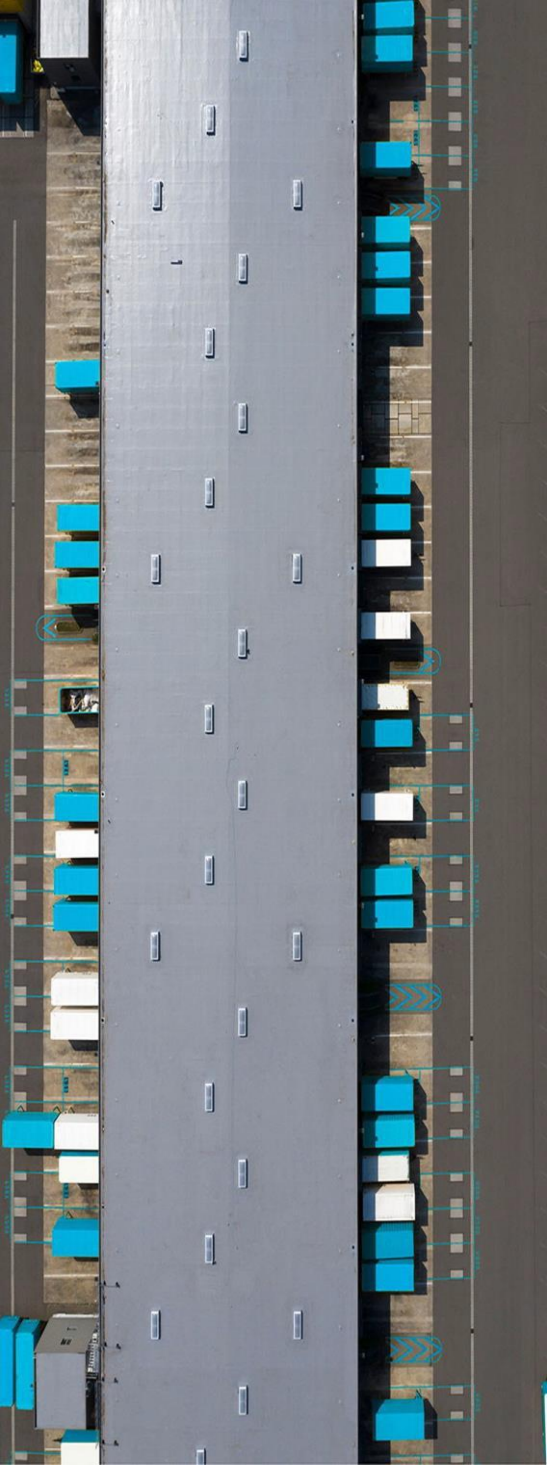
Blue Yonder Security Whitepaper

BLUE YONDER WHITEPAPER | November 2023 | Version 3.0

BlueYonder

Table of Contents



BlueYonder

Security Overview

Blue Yonder understands to retain, attract, and grow our business, customers must place their trust in us to do what we say we are going to do. It starts with building secure software solutions and delivering secure cloud services that protect our customers' data.

We are constantly evaluating procedures, processes, and controls to best honor our commitments to our customers. The investments we make in people and training, through Associate Success, and technology are integral for protecting business assets, securing information, and streamlining processes.

The contents of this white paper are a summary of the depth and breadth of Blue Yonder's Cybersecurity Program, sponsored by Executive leadership.

Additionally, this white paper is designed to give you an overview of our customer commitment.

It begins with trust.

Organizational Security

Associate Success

Blue Yonder has re-defined the way it supports its associates through Associate Success. Associate Success is a holistic approach that includes security elements throughout the associate lifecycle from screening, onboarding, employment and through separation processes.

As stated in the Associate Handbook:

"Our core values unite and inspire us. They are ingrained in every interaction with a customer, partner, and each other. We hold each other accountable for living these values and seek to engage others who embrace our emphasis on **empathy** towards others, **teamwork**, **relentless** learning, and a focus on delivering **results**."

Blue Yonder culture is rooted in its values.

Values are reinforced by Executive leaders setting the example by communicating strategy and key messages with transparency—routinely and company-wide. The Blue Yonder strategy is put into practice through a robust set of policies, standards, processes, and procedures.

Dedicated Cybersecurity Team

The Cybersecurity Team is comprised of the following:

Cybersecurity Governance, Risk & Compliance
Cybersecurity Threat & Vulnerability Management
Cybersecurity Architecture & Engineering
Cybersecurity Awareness, Training & Education
Cybersecurity Operations

This team exists to identify and protect against threats before they occur; and detect, respond, and recover from any potential security incidents. The Cybersecurity Team partners with all business units of the organization to provide awareness, education, resources, and best practices to ensure a safe and secure environment for our associates, partners, and customers.

Access Control

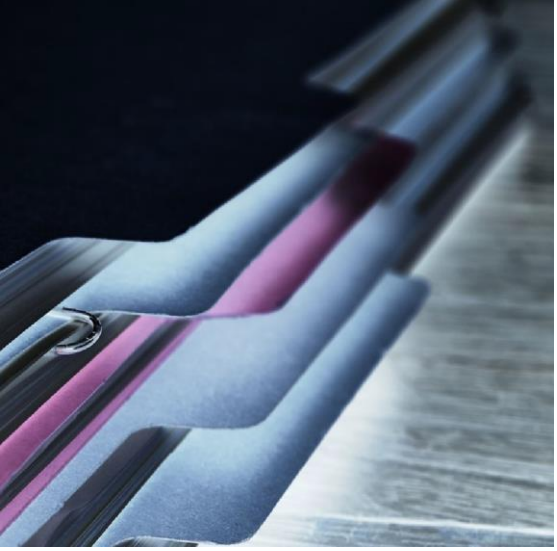
Blue Yonder maintains a number of technical and organizational controls designed to ensure separate users and processes are based on different levels of trust, needs, and privilege requirements. This means that users, the network, or services will have only the minimum access privileges necessary to perform a specific job or task and nothing more.

Access, authentication, and authorization controls are designed to ensure there are role-based access privileges and authentication measures in place. Access to production servers, database servers, network domains, and resource groups, is role-based and restricted to authorized personnel.

Each user is identified by a unique user ID. The use of generic/ shared IDs for system access is not permitted. Users are required to authenticate through their unique user ID and password for each domain. Users are required to use complex passwords of at least 8-character length (including upper case, lower case, numerical value, and a special character) which expires every 90 days. Password reuse is set to 24.

User access is reviewed annually, and inactive accounts are automatically disabled after 90 days and deleted after 120 days of dormancy. System access privileges are automatically revoked as a component of the termination process.

Blue Yonder Cloud Services utilizes Multi-Factor Authentication (MFA) for all administrative access. Administrative user account passwords are securely stored in a password vault. The passwords are changed every day for privileged accounts, so these accounts will not be auto disabled or deleted. Privileged user access for cloud infrastructure is reviewed on a quarterly basis to ensure that access to critical systems is restricted to authorized personnel.



Background Checks, Onboarding and Separation

Blue Yonder utilizes external agencies to perform background checks for all new and contingent workers in accordance with local laws, regulations, ethics, and contractual constraints.

During the onboarding process, associates, and contingent workers are required to sign a code of conduct, confidentiality agreement and acknowledge their understanding of the cybersecurity policies.

Associates who violate the cybersecurity policies are subject to disciplinary actions up to and including termination of employment. Additionally, a Non-Disclosure Agreement is signed as part of separation from the company.

Security Awareness Training

As part of the onboarding process and annually thereafter, all Blue Yonder associates and contingent workers are required to take a series of courses including security and privacy. Depending on the job role, additional training on specific aspects of security may be required. The training aligns with the NIST SP 800-53r5 and ISO 27001 compliance frameworks and reinforces the business objectives and culture of the organization.

It is designed to help associates understand potential cybersecurity risks, including phishing, social engineering, and data privacy. The material leverages learning principles to enhance content retention and are regularly updated as digital attack techniques evolve.

Protecting Customer Data

Secure by Design

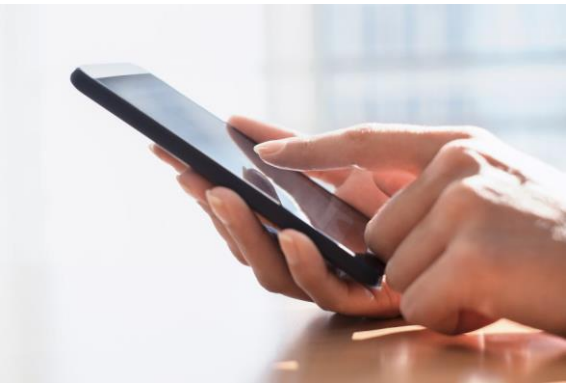
Security best practices are integrated into every aspect of the software development process. Developers build secure software using guidance including the OWASP Top 10. Additionally, interactive training is available in specific development languages which reinforces the overall security posture and culture related to coding and development.

Software development at Blue Yonder adheres to the Secure Software Development Life Cycle (SSDLC). In addition to secure code testing and open-source testing, Blue Yonder performs dynamic application security testing (DAST) to test for web application vulnerabilities, and static application security testing (SAST) to identify client-side vulnerabilities. Vulnerability scans are performed, and a manual internal penetration test is per- formed before application release.

Encryption

Blue Yonder uses industry approved encryption technologies to protect communications and operational processes including customer data in transit and at rest.

Encryption of data in transit is via HTTPS, SFTP or AS2 using TLS 1.2 or higher. Data at rest is encrypted using AES256 bit encryption at the disk array. Database encryption is implemented based on the ability of the solutions and customer requirements.



Infrastructure Security

Infrastructure security is key to Blue Yonder Cloud Services. Blue Yonder cloud infrastructure is hardened to industry accepted benchmarks. Cloud infrastructure servers are patched monthly to ensure maximum compliance with vendor patches. Monitoring systems are in place and alerts are triggered on the operational performance and capacity levels of Blue Yonder systems. The alerts automatically generate a tracking ticket and are assigned to the appropriate stakeholders to take appropriate action. Blue Yonder cloud infrastructure can be administered only through Blue Yonder owned and managed devices with standard endpoint security configurations.

Network Security

Blue Yonder cloud networks are separated from internal and external networks with firewalls. Blue Yonder associates and contingent workers are provided with laptop and VPN access with multi-factor authentication to securely connect to the company network. Administrators can access Blue Yonder cloud infrastructure only through the Blue Yonder network and cannot access it through public channels. Access to customer environments require an additional VPN and multi-factor authentication.

Each customer environment is segregated with a separate firewall context. Cloud Services uses an Intrusion Detection System/Intrusion Prevention System (IPS/IDS) solution to examine network traffic flows and to detect/prevent network-based attacks. A third-party service is used to monitor and react to network related threats including DDoS attacks. Blue Yonder works with network carrier providers to leverage their capabilities in identifying and mitigating network attacks.

Endpoint Security

Blue Yonder endpoints (including laptops) and servers are equipped with Endpoint Detection and Response (EDR) software. Signatures for the anti-malware software are updated daily to receive any urgently required patches. Installation of unauthorized software is not allowed.

Customer Access Control

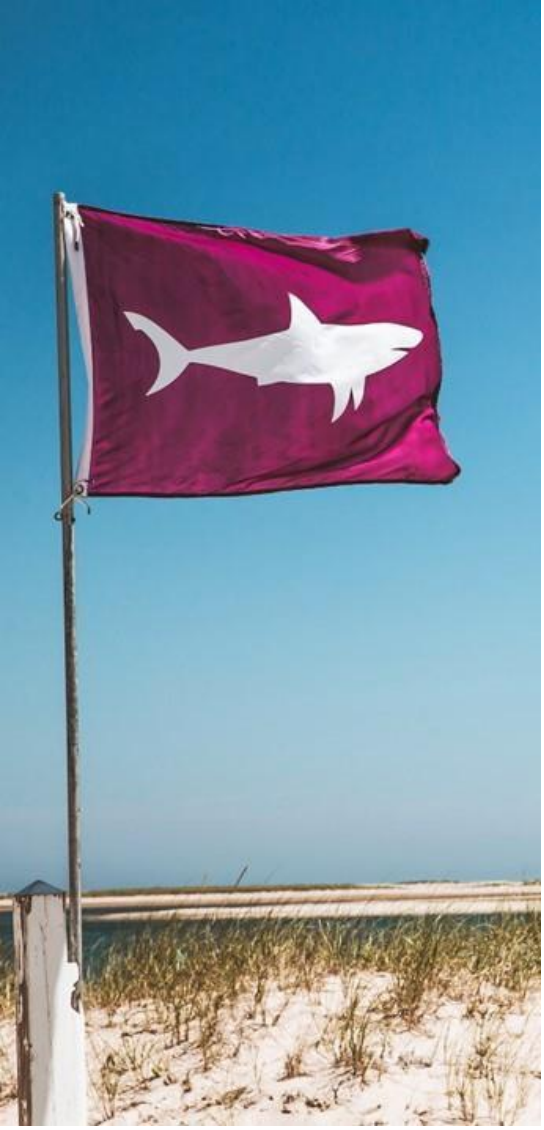
Data Protection is vital to Blue Yonder. Customers own their data. Data protection begins with access based on data classification. Blue Yonder classifies data as either Restricted, Confidential or Unrestricted. All customer data is classified as Confidential.

For solutions where Blue Yonder Cloud Services administers user access, an authorized customer representative is required to submit an access request through the ticketing system. It is the customer's responsibility to ensure that the request has been properly reviewed and approved to comply with the customer's business process and access control guidelines. This includes the disabling of access for terminated associates and changes in role and access. For Blue Yonder Cloud Services solutions where the customer directly administers user accounts, the authorized customer representatives have access to the user administration functions of the application.

Identity and Access Management

LIAM is a core component of Blue Yonder's supply chain platform focusing on customer-facing identity access management. The Luminate IAM Service (LIAM) is built on Azure AD B2C technology which is a Microsoft identity-as-a-service (IDaaS) product that can broker various supported identity providers (SAML2, OpenID Connect/OAuth2) and produce a normalized identity and access experience that applications can then consume in a standard manner (OpenID Connect/OAuth2). It provides centralized identity access management for customers' identities. Enabling customers to use their own (corporate) identities in Blue Yonder's product via federation.

Single Sign On (SSO) options are also available. Authentication and SSO functions can be federated or delegated to LDAP, Active Directory or any system supporting SAML 2.0 and OpenID Connect protocols. Multi-factor authentication is supported by the Blue Yonder applications; however, it needs to be managed by customer's authentication provider along with SSO.



System Monitoring, Logging, and Alerting

At Blue Yonder, changes to operating environments are logged, monitored, and reviewed. Logging facilities and log information are protected against tampering and unauthorized access. Blue Yonder Cloud Services leverages a centralized 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 by a vendor managed Security Operations Center (SOC). The SOC team identifies security events and notifies the Blue Yonder security team with recommended actions. Log files cannot be exported from the SIEM and are not shared with customers.

Vulnerability Management

Vulnerability management encompasses identifying, categorizing, prioritizing, and resolving vulnerabilities in operating systems, cloud and on-premises enterprise applications, browsers, and end-user applications. Through monthly scanning, asset owners are notified of new and actively exploited vulnerabilities to review and remediate.

In the case of zero-day threats, systems are scanned immediately, and the SOC team is notified of potential compromises and prepare remediation actions.

Patch Management

Patching is a normal part of operating the business. Blue Yonder tests and applies patches based on criticality. Through customer coordination, Blue Yonder Cloud Services keeps the customer environments (test, development, production) updated with patches and upgrades.

Penetration Testing

Blue Yonder products go through manual internal penetration testing to detect and address vulnerabilities prior to release. External infrastructure penetration testing is performed annually by third parties on cloud infrastructure environments.

Data Retention and Disposal

Blue Yonder utilizes data classification levels to define the level of protection required throughout its lifecycle. Data is removed using secure methods before media retirement and disposal. Evidence is maintained of data cleansing activities. Customer data is securely disposed of within 30 days after the termination of the contract.

Availability, Disaster Recovery and Business Continuity

Blue Yonder application servers are deployed in a cluster environment within multi-tier distributed scenarios. This eliminates a single point of failure and allows for high availability.

Standard Availability SLA levels are maintained at 99.7% which is a testament to our resilient systems and processes. (Available means the percentage of time in a calendar month that the applicable Cloud Services are accessible for production use.)

Business continuity and disaster recovery are dependent upon operational resilience and preparation. Assurances to mitigate business interruptions are provided for every customer production environment and are defined based on customer preferences.

Blue Yonder Cloud Services offers different recovery options for customers based on a range of recovery levels (RTO – Recovery Time Objective and RPO – Recovery Point Objective). The standard RTO is up to 48 hours and the standard RPO is 4 hours. The Extended Plus option for RTO is 8 hours and the RPO is 1 hour.

Backup Processes

Blue Yonder provides highly capable automated backup mechanisms at defined internals to support a range of customer requirements for public and private cloud product offerings. Backups are retained for 30 days, unless otherwise dictated by customer requirements. Backup data is stored onsite, encrypted at-rest at the array level using 256-bit encryption. A copy is kept offsite for redundancy, is also encrypted at the array level.

Change Management

Blue Yonder employs a change management process to manage, monitor, and successfully execute change requests. Impact and risks are assessed for each request, and appropriate rollback plans are prepared before implementing changes. Changes are tested in non-production environments before they are promoted to production. Review and approvals are managed through the Change Control Board.

Responding to Security Incidents

Cybersecurity Incident Management encompasses the Cybersecurity Incident Response Policy, the Cybersecurity Incident Response Team ("SIRT"), and the Cybersecurity Incident Response Plan (IRP). The SIRT establishes and maintains capabilities to respond effectively to electronic network intrusions.

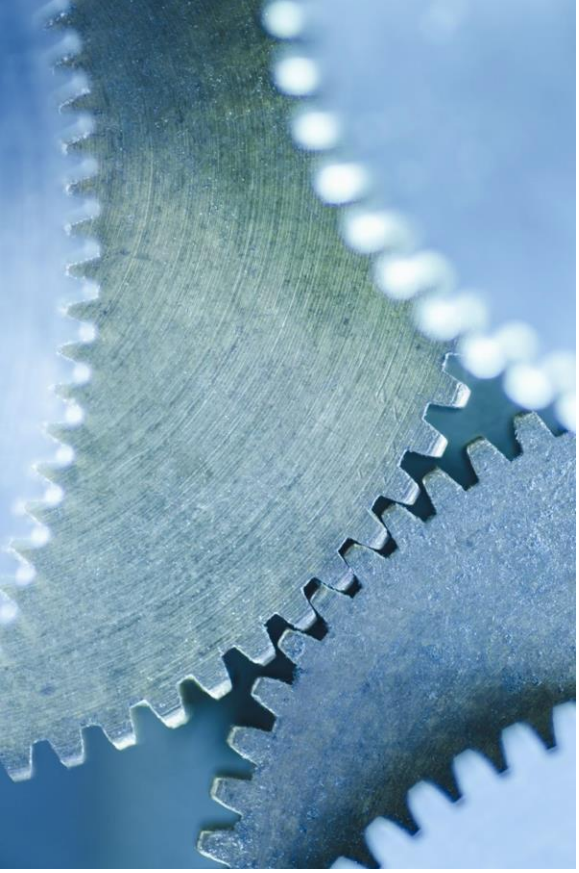
Incidents are assigned a Severity Level from 1 (highest) to 4 (lowest) based on the technical and business impact of the reported problem.

Cybersecurity incident management includes 24-hour monitoring and provides support and escalation for customer production systems.

Physical Measures

Blue Yonder datacenters have multiple layers of protection to control access to resources, including tapes and backup media. Layered physical security measures begin with access approval at the facility's perimeter, at the building's perimeter, inside the building, and on the datacenter floor. All servers are housed in a Blue Yonder managed or directly subcontracted data center (with similar level of security requirements). Data center security features include:

- 24 X 7 security cameras with recordings, monitored onsite.
- Alarms for emergency doors, forced door open alerts, etc.
- Associate access is limited and restricted by job function.
- Proximity badges are required for entry.
- Access activities are logged, reviewed, and audited.
- Visitor access is strictly controlled; visitors are always escorted.



Vendor Management

Third-Party Risk Management (TPRM)

Each third-party service provider is expected to comply with Blue Yonder mandated security policies and are responsible for any subcontractors. Prior to on-boarding, security requirements are established and agreed upon with each service provider that may process, store, or transmit Blue Yonder information. All third-party service providers undergo the following:

- ☑ Vendor Onboarding and Offboarding Process Flows
- ☑ Inherent Risk Scoring
- ☑ Vendor Criticality Categories
- ☑ Ongoing Monitoring Cadences

- Risks are identified, assessed, remediated, and actioned as needed through the Third-Party Risk Assessment process.
- Data Privacy Impact Assessments are performed as needed.
- Contracts are reviewed by Legal and Security with consideration given to global legal and regulatory requirements.
- Vendors undergo periodic reassessments dependent upon the associated risk level.

Blue Yonder monitors supplier performance on a regular basis against established SLAs.

Service providers are required to report to Blue Yonder any incident impacting or involving Blue Yonder data or assets.

Compliance, Audit and Validation

Compliance Audits

Cybersecurity Compliance plays a critical role in providing assurance for customers and is an important element in building customer trust relationships. Through rigorous and industry recognized standards, Blue Yonder is audited and certified by an independent third party. Blue Yonder maintains multiple security certifications and attestations by undergoing regular third-party audits of the cloud services offerings, including:

SOC 1 Type 2
SOC 2 Type 2
ISO 27001 (Security)
ISO 27701 (Privacy – Certification in December 2022)
ISO 22301 (Business Continuity – Certification in 2023)

Customer Driven Audits

Annually customers may submit control questionnaires for completion by the Compliance team. This activity is usually prompted by new or prospective business, or annually as part of a customer's own vendor management processes.

Customers may email security@blueyonder.com to request compliance reports or submit security questionnaires.

Appendix

Global Workplace - Securing Our People

Acceptable Use Policy
Business Continuity Policy
Cryptography Policy
Cybersecurity Policy
Incident Response Policy
Cybersecurity Risk Management Standard
Systems and Services Acquisition Policy

Acceptable Use Policy		
1.0	Purpose	The Acceptable Use Policy defines the company objectives for establishing specific standards on the appropriate business use of the company's information and telecommunications systems and equipment.
2.0	Scope	All individuals, groups, or organizations ("Users") identified in the scope of this Policy are responsible for familiarizing themselves and complying with the Acceptable Use Policy and associated standards and guidelines.
3.0	Policy	Company provided assets are provided for official and authorized company business purposes only. Blue Yonder reserves the right to monitor, record, or periodically audit use of any of its information and telecommunications systems and equipment.
4.0	End-User Computing and Technology Requirements	Company technology-based resources are provided for official and authorized company business use and purposes in support of the company's mission. Users must ensure passwords meet the following criteria: Standard password length must be eight characters or longer. Administrative password length must be eight characters or longer. Passwords must contain at least three of the following four characteristics: 1 uppercase alphabetic, 1 lowercase alphabetic, 1 special character and 1 numeric character.
5.0	Internet Acceptable Use	Company technology resources are provided for official and authorized company business use and purposes. Limited, reasonable private use of technology resources are acceptable.
6.0	Software Acceptable Use	Users cannot use software that has not been approved by Information Security.
7.0	BYOD Acceptable Use	If the BYOD technology cannot meet requirements, the device will not be permitted to connect to company resources. Any processing, storage or transmission of company information must be conducted on company owned resources.
8.0	Electronic Mail Acceptable Use	Company electronic mail resources are provided primarily for official and authorized company business use. Limited private use of company electronic mail resources is acceptable if it does not interfere with normal business operations.
9.0	Material Non-Public Information Use	Associates, contingent workers, and users may be exposed to confidential and other material, non-public information of the company or its affiliates, partners, suppliers, customers, or third parties. If exposed to such material, one must not act upon the information in terms of security trading or disclosure of confidential information.
10.0	Ownership and Responsibilities	Senior management and department managers are accountable for ensuring that the Acceptable Use Policy and procedures are properly communicated.
11.0	Enforcement	Failure to comply with the Acceptable Use Policy and associated guidelines and procedures can result in disciplinary actions.
12.0	Definitions	Terms that are not covered in other key policies are detailed in this Section.

Business Continuity Policy		
1.0	Purpose	The Business Continuity Policy states requirements to counteract interruptions to business activities during an outage or disaster.
2.0	Scope	All Associates, Contingent Workers, and those employed by others to perform work on company premises or who have been granted access to company information or systems, such as customers and their end-users, are covered by this Policy and must comply with associated requirements and procedures.
3.0	Policy	Business continuity plans are maintained which identifies critical business functions along with their business continuity requirements. Business teams provide Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO). The Business Continuity Plan documents stakeholders, roles, responsibilities, and procedures.
4.0	Ownership and Responsibilities	Senior management and department managers are accountable for ensuring that the Business Continuity Policy and procedures are properly communicated.
5.0	Enforcement	Failure to comply with the Business Continuity Policy and associated guidelines and procedures can result in disciplinary actions.
6.0	Definitions	Terms that are not covered in other key policies are detailed in this Section.

Appendix – Cryptography Policy		
1.0	Purpose	The Cryptography Policy describes the requirements for protecting, through various encryption methodologies, the confidentiality and integrity of data as it traverses' networks or as it is stored within systems.
2.0	Scope	All Associates, Contingent Workers, and those employed by others to perform work on company premises or who have been granted access to company information or systems, such as customers and their end-users, are covered by this Policy and must comply with associated policies and procedures.
3.0	Policy	Encryption is implemented and maintained by appropriately trained, role-based associates, for use by users to protect the confidentiality and integrity of sensitive company information assets.
4.0	Approved Encryption Algorithms	The Cryptography Policy sites specific sources for suitable and approved cryptographic algorithms such as the IETF RFC Guide.
5.0	Ownership and Responsibilities	Senior management and department managers are accountable for ensuring that the Cryptography Policy and supporting procedures are properly communicated.
6.0	Enforcement	Failure to comply with the Cryptography Policy and associated guidelines and procedures can result in disciplinary actions.
7.0	Definitions	Terms that are not covered in other key policies are detailed in this Section.

Appendix – Cybersecurity Policy		
1.0	Purpose	This Policy, is to provide management direction and support for information security in accordance with the business requirements of the company and applicable laws, contractual requirements, and regulations.
2.0	Scope	All associates, contingent workers, and those employed by others to perform work on company premises or who have been granted access to company information or systems, are covered by this policy, and must comply with associated guidelines and procedures.
3.0	Objectives	The cybersecurity objectives form a holistic perspective and are addressed in numerous policies and standards.
4.0	Ownership and Responsibilities	The head of Cybersecurity Governance, Risk and Compliance is responsible for the development, implementation, and maintenance of the Cybersecurity Policy and associated standards and procedures while the Chief Security Officer authorizes the approval of the Cybersecurity Policy, standards, and associated procedures.
5.0	Enforcement	Failure to comply with the Cybersecurity Policy and associated guidelines and procedures can result in disciplinary actions.
6.0	Definitions	Terms that are not covered in other key policies are detailed in this Section.

Appendix – Cybersecurity Risk Management Standard		
1.0	Purpose	The Cybersecurity Risk Management Standard ensures risk management activities are centered on transparent communication and rapid deployment of resources.
2.0	Scope	All associates, contingent workers, and those employed by others to perform work on company premises or who have been granted access to company information or systems, are covered by this policy, and must comply with associated guidelines and procedures.
3.0	Policy	This standard ensures that the risk management methodology is consistent with NIST Special Publication 800-37. This Framework is a holistic, organization-wide cycle of risk management that integrates security risk categorization, design, assessment, authorization, and monitoring practices into information systems to facilitate risk- based decisions.
4.0	Ownership and Responsibilities	Senior management and department managers are accountable for ensuring that the Cybersecurity Risk Management Standard and supporting procedures are properly communicated.
5.0	Enforcement	Failure to comply with the Cybersecurity Risk Management Standard and associated guidelines and procedures can result in disciplinary actions.
6.0	Definitions	Terms that are not covered in other key policies are detailed in this Section.

Appendix – Incident Response Policy		
1.0	Purpose	The Incident Response Policy solidifies the requirement to ensure security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.
2.0	Scope	The Security Incident Response Team (SIRT) will establish and maintain capabilities to respond effectively to electronic intrusions into the Company network infrastructure.
3.0	General Requirements	The SIRT will maintain plans for responding to typical types of intrusion vents as well as processes for responding to new or unanticipated types of intrusions.
4.0	Response Requirements	The SIRT verifies the existence of network and system intrusions and takes actions to contain the threat in accordance with the response plan.
5.0	Recovery Requirements	The SIRT team will assess any damages and coordinate with Company departments or teams responsible for recovering impacted systems. Lessons learned will be documented.
6.0	Ownership and Responsibilities	Core SIRT members are designated representatives from key Company departments that have primary responsibility for performing SIRT routine operations and Incident response efforts.
7.0	Enforcement	Failure to comply with the Incident Response Policy and associated guidelines and procedures can result in disciplinary actions.
8.0	Definitions	Terms that are not covered in other key policies are detailed in this Section.

Appendix – Systems and Services Acquisition Policy		
1.0	Purpose	The Systems and Services Acquisition Policy ensures that effective, appropriate, and consistent levels of security and service delivery are implemented within contracted services from vendors, partners and other third parties.
2.0	Scope	All associates, contingent workers, and those employed by others to perform work on company premises or who have been granted access to company information or systems, are covered by this policy, and must comply with associated guidelines and procedures.
3.0	Policy	Vendors must undergo a due diligence check which entails a third-party risk assessment, data privacy impact assessment (as appropriate), and a legal review of the vendor contracts.
4.0	Ownership and Responsibilities	Senior management and department managers are accountable for ensuring that the Systems and Services Acquisition Policy and supporting procedures are communicated.
5.0	Enforcement	Failure to comply with the Systems and Services Acquisition Policy and associated guidelines and procedures can result in disciplinary actions.
6.0	Definitions	Terms that are not covered in other key policies are detailed in this Section.

About Blue Yonder

Blue Yonder, Inc. (formerly JDA Software, Inc.) provides seamless, friction-free commerce, empowering every organization and person on the planet to fulfill their potential. Blue Yonder's machine learning-driven digital fulfillment platform enables clients to deliver to their customers when, how and where they want it. Applying over 35 years of domain expertise, contextual intelligence, and data science, Blue Yonder is helping more than 3,300 of the world's leading manufacturers, retailers and logistics companies create more autonomous, sustainable, and profitable operations.