BLUJAY SOLUTIONS

Information Security

OVERVIEW

Contents

DISCLAIMER

The information provided herein by BluJay Solutions and/or its affiliates is provided for informational purposes. The information is complete and accurate to the best of BluJay's knowledge as of the published date and is subject to change. BluJay makes no representations, guarantees, or contractual commitments by providing the information herein. The information contains confidential and proprietary information of BluJay and provides an overview of the BluJay products and services. BluJay makes no commitment or promise to deliver any material, code or functionality referenced herein and the development, release and timing of any product features and functionality remains at the sole discretion of BluJay.

VERSION 02

BluJay Security Overview

BluJay's purpose is to transform supply chains into frictionless, high-performance and high-value assets by delivering a blend of Data, Networks, and Applications — it's in our DNA.

The BluJay Way is to empower greater adoption and deliver more value through our people and services. At BluJay we believe that ensuring the confidentiality, integrity, and availability of our customers' systems and data is of the utmost importance, as is maintaining customer trust and confidence. Handling the privacy and security of information is a vital part of our responsibility to our clients and essential to our success as an organization.

BluJay understands the importance of taking appropriate steps to safeguard our internal and customer information and is committed to protecting it from unauthorized use and disclosure. We keep security top of mind in all areas from the design, development, integration, processing and overall collaboration of our products and services.

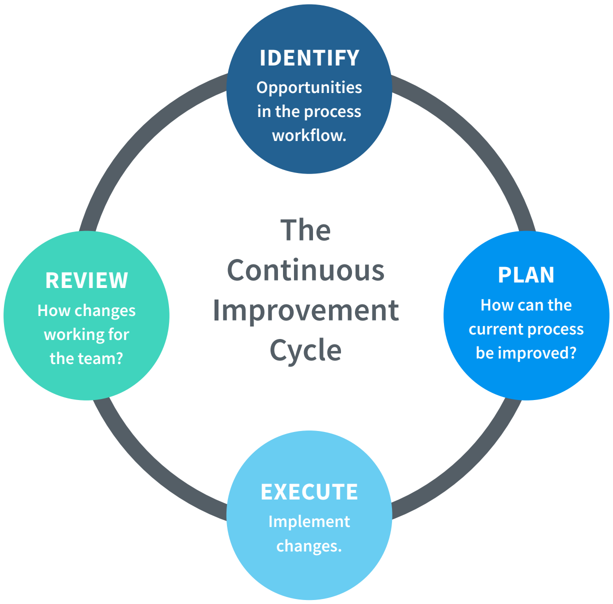
Our global interfaces are backed by an adaptable network infrastructure, which allows us to work more fluidly while also working behind the scenes to provide our clients and 50,000 connected partners with fast and reliable solutions that best meet the needs of establishing a strong security foundation.

BluJay's Security Team

As part of BluJay's commitment, we have a dedicated global information security team focused on delivering secure solutions and environments for our customers.

Our team operates globally and supports all facets of information security including protecting information, applications, and our infrastructure. BluJay's Vice President of Information Security has overall responsibility for BluJay's information security program, security strategy, policy, and architecture, and reports to an internal executive governing body.

BluJay's governing body is a cross-functional group representing Legal, HR, IT, and Executive Leadership. This team is also part of the Global Security Incident Response Team (GSIRT) in the event of a security incident.


IDENTIFY
Opportunities in the process workflow.
PLAN
How can the current process be improved?
EXECUTE
Implement changes.
REVIEW
How changes working for the team?
The Continuous Improvement Cycle

Compliance

BluJay's Governance, Risk, and Compliance framework is based on governance-focused industry standards, comprised of a robust set of controls that make up our internal Information Security Management System (ISMS), ensuring applicable audit compliance standards are met.

The IT infrastructure and solutions that BluJay provides to its customers are designed and managed in alignment with security best practices and a variety of IT security standards, including:

Certifications

- BluJay certifications include ISO 27001:2013 for our German and Swiss locations and SSAE16 SOC I Type II for our Transportation Management for Shippers solution.
- Third-party data center partners hold multiple certifications, including ISO 27017, 27018 and PCI.

Partners

- BluJay works with strong, industry-leading global providers and vendors.
- Vendors are assessed and subject to BluJay's security, compliance, and data protection requirements.

Training and Awareness

- BluJay provides global employee training on data security, privacy, ethics, and targeted training initiatives to ensure adequate topics are covered and acknowledged by our employees.
- Role-based focused training for key functions, e.g. secure coding training for product developers.

Continuous Improvement

- BluJay is committed to ongoing enhancements to business processes, services, contracts, and policies to support data security and compliance with all applicable laws.
- BluJay has an established ITIL based Change Management Program that includes:
  - **Development:** Unit Testing, Module Testing, Code Quality/Static Analysis
  - **QA:** System Integration Testing, Regression Testing, Scalability and Performance Testing, Security Testing
  - **Customer Testing / Acceptance:** UAT

GLOBAL ISMS AND SUPPORTING INTERNAL POLICIES AND PROCEDURES

BluJay maintains a Global ISMS policy set that defines the different control areas and domains for securing our data, assets, and information. BluJay reviews this annually in support of the Global ISMS program.

The Global ISMS policy set is governed by an overarching Global Information Security Policy which defines the hierarchy and delineates the security domains of the supporting policies. The Global ISMS policy set aligns to industry best practices such as NIST and the ISO 27001:20013 framework and includes the following:

Global Information Security Policy

1. Acceptable Use Policy
2. Clean Desk Policy
3. Access Control Policy
4. Vulnerability Management Policy
5. Physical Security Policy
6. Personnel Security Policy
7. Information Classification and Handling Policy
8. Encryption Policy
9. Network Security Policy
10. Secure Development Policy
11. Security Monitoring and Response Policy
12. Data Disposal and Destruction Policy
13. Bring Your Own Device Policy
14. Change Management Policy
15. Antivirus Policy
16. Acceptable Use Policy
17. Business Continuity Policy
18. Vendor Security Policy
19. Password Policy

Additional policies which support the overall ISMS program for the Global Information Security team include:

- Global Training Policy
- Incident Response Plan
- Risk Assessment and Treatment
- Risk Exception Policy

PRIVACY AND DATA PROTECTION

BluJay is committed to respecting the privacy of personal information that is shared with us, directly or indirectly, in connection with our customers' use of our products and services.

BluJay partners with an external Data Privacy Organization that specializes in international data regulation and ethics. This ensures a multi-disciplinary team of data protection practitioners, lawyers, corporate governance, and cyber security experts with a wealth of data protection and privacy knowledge.

BluJay complies with the frameworks and recommendations set forth by the U.S. Department of Commerce and European Data Protection Board (EDPB) on measures regarding the collection, use, and retention of personal information and data classification according to regional regulations.

To view BluJay's full Privacy Policy please visit:
https://www.blujaysolutions.com/privacy-policy/

GENERAL DATA PROTECTION REGULATION (GDPR)

GDPR is a comprehensive data protection law in the EU that is designed to unify data privacy requirements across the EU. The GDPR is directly enforceable in each EU member state.

The GDPR regulates the "processing" of data for individuals (called "data subjects") in the EU. Processing can mean collection, storage, transfer, or use of data and organizations need to ensure they have a lawful basis for processing such personal data. Also important is that GDPR defines "personal data" broadly; it covers any information relating to an identified or identifiable data subject.

As part of BluJay's commitment to our customers, BluJay only processes data in accordance with customers' instructions for purposes of providing the agreed solution and services. Furthermore, any processing is in compliance with the applicable data protections laws and regulations, including GDPR.

For more information on
BluJay's approach to GDPR please visit:
https://www.blujaysolutions.com/
gdpr-data-security-blujay/

Business Impact / Risk Assessment & Treatment

BluJay applies risk assessment and treatment to the entire scope of the Information Security Management System (ISMS) (i.e. to all assets which are used within the organization or which could have an impact on information security within the ISMS).

BluJay conducts a business impact assessment (BIA) at least annually to identify critical processes, assess the potential impact of disruptions, set prioritized timeframes for recovery, and identify critical dependencies and suppliers. Additionally, BluJay conducts company-wide risk assessments, at least annually, to help us systematically identify, analyze, and evaluate the risk of disruptive incidents to BluJay. Identification of information assets and final assignment of risk is performed with input from the business and risk treatment is identified accordingly. Together, the risk assessment and BIA drive continuity priorities, and mitigation and recovery strategies for our business continuity plans (BCPs).

BluJay conducts a business impact assessment (BIA) and a company-wide risk assessment at least annually

HR, Training, & Awareness

BluJay's Global Security team partners with our Human Resources and Legal teams to define and conduct company-wide training to help ensure compliance and user acknowledgment in all security related areas.

As a critical line of defense in keeping organizational information and systems secure, it is vital that our users (full-time employees, contractors, and business partners) understand how their individual day-to-day actions directly reflect upon the company's and client's overall security posture.

BluJay's primary goal is to reduce the risk of information loss, leakage or exposure through human error via inadvertent or deliberate action. We accomplish this by establishing and fostering a "security culture" where EVERYONE is an actively engaged participant where security is "top of mind" and where correct security-related behaviours are enforced.

BluJay conducts regular, compulsory training for all employees on data security, data privacy, and a number of other areas, such as anti-bribery and whistle-blowing etc. Training programs require employees to acknowledge internal policies in alignment with the training materials.

ONBOARDING/OFFBOARDING

BluJay's Human Resources team maintains strict processes for effective onboarding and offboarding of team members. From a security perspective this includes:

Onboarding:

- Pre-employment background checks (subject to national, regional, local regulations and position)
- Non-disclosure and confidentiality agreements
- Security training program
- Allocation and registration of assets (e.g. laptop, mobile phone)

Offboarding:

- Notification to relevant departments
- Return of assets
- Removal of digital access (logins, email, etc.)
- Ensuring data disposal and destruction for customer related information

> **BluJay's primary goal is to reduce the risk of information loss, leakage or exposure through human error via inadvertent or deliberate action.**

Infrastructure Security

BluJay protects its computer systems and information storage facilities against the unauthorized destruction, loss, alteration of, or access to information. This includes the use of data centers in secure facilities that are carrier-neutral and provide physical security, redundant power, and infrastructure redundancy. BluJay requires its internet service providers to ensure a high level of uptime and have a rapid failover capability.

As a company operating with a wide global footprint, BluJay secures corporate and production systems via:

THIRD-PARTY DATA CENTERS

Third-party service providers are responsible for the physical, environmental, and operational security controls at the boundaries of BluJay infrastructure.

BluJay is responsible for the security of the physical and logical compute, networks and applications, used to provide the services hosted at third-party data centers.

Security controls at third-party subservice organization data centers include:

- Accreditations, vendor security questionnaires, contract and contractual SLA commitments
- Annual review of security controls
- Strictly controlled physical access both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means
- Authorized staff must pass two-factor authentication a minimum of two times to access data center floors
- All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff
- Data center access is only granted to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, access is immediately revoked, even if they continue to be an employee of BluJay

THIRD-PARTY CLOUD SERVICE PROVIDERS

Cloud Service providers are responsible for securing the infrastructure that runs all of the services offered in the Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run the Cloud services. Connections are protected through their firewalls, which are configured in a default deny-all mode.

BluJay restricts access to the environment to a limited number of IP addresses and employees.

ACCESS CONTROL

Access rights within BluJay are based on the user's role and are defined based on "least privilege" and "need-to-know."

Procedures are in place to prevent our data processing systems from being used by unauthorized persons including:

- Identification of the terminal and terminal user to the BluJay systems
- Firewall, router, and VPN-based access controls to protect the private service networks and back-end-servers
- Role-based access controls (requests are submitted through internal approval systems and approved by an appropriate authority)
- Logged access to host servers, applications, databases, routers, and switches
- Strong password requirements and use of multi-factor authorization

Information Security

BluJay leverages a defense in depth approach to help ensure networks and systems are adequately protected. BluJay utilizes a number of industry-standard tools and protection techniques, along with defined processes to help ensure a robust system of control exists for our infrastructure. This includes firewalls, network vulnerability scanning, network security monitoring, and intrusion detection and prevention systems so only eligible and non-malicious traffic is able to reach our infrastructure.

Our internal networks are segmented and tiered, and access is controlled throughout the environment allowing only those connections necessary within the environment.

NETWORK HARDENING STANDARD

BluJay has established a security standard related to Network Infrastructure Element Hardening for ongoing operations and support of BluJay Global Security Policies.

The standard describes the minimum requirements and practices that must be followed when configuring a network infrastructure element and applies to all environments, systems, applications and applicable technologies connected to the BluJay infrastructure, or otherwise utilized by BluJay.

VULNERABILITY MANAGEMENT

BluJay's Vulnerability Management program provides a global service that addresses security risks to ensure clear processes and accountability for the identification, notification, remediation, and reporting of vulnerabilities.

Our Global Information Security team conducts due diligence and thorough security testing (including dynamic and static, internal and external scanning) within the BluJay environments. The team also takes the identification of known threats and vulnerabilities into consideration while proactivity working to remediate and protect our assets to the best of our ability.

THIRD PARTY TESTING

BluJay partners with third-party providers to perform penetration testing of our networks and applications. All testing is performed using industry standard tools and third-party partners to identify security vulnerabilities and bugs using proven techniques. e.g. external and internal scanning, penetration testing, static and dynamic code testing, etc.

Output of these activities and testing cadence are regularly reviewed by the global information security team, along with key business and IT personnel to define scope of testing, validate results and prioritize remediation, in line with our contractual obligations to our customers.

DATA PROTECTION AND ENCRYPTION

Securing and protecting data in transit and at-rest is of significant importance to BluJay. BluJay supports strong encryption methods to secure connections between our customers and our networks, as well as encrypting data at-rest.

BluJay has a defined Encryption and Key Management Standard that sets forth the acceptable cryptography standards for use across BluJay systems and environments. This standard exists to address issues and provide clarification related to encryption by identifying specific requirements that information resources must meet for BluJay.

Additionally, customer data is appropriately segregated and protected across BluJay's database instances.

LOGGING AND MONITORING

BluJay uses a series of enterprise and proprietary tools to monitor network, storage, servers, virtual hosts, and applications to help ensure systems are operating as intended.

Logs are collected and where appropriate centralized and retained for use by authorized personnel.

ANTIVIRUS & ANTIMALWARE

BluJay utilizes industry standard tools and techniques to adequately monitor and protect against viruses and malware, by maintaining up-to-date protection across our systems.

Application Security

SECURE DESIGN PRINCIPLES

BluJay recognizes the importance of integrating security at the conception of all projects, services, and partnerships. Security analysis begins at the design phase, is continuously conducted throughout the entire development process, and aligns to best-practice methods such as static code analysis, standard build process and evaluation of risk, all of which assist in limiting the identification of issues that could incur additional cost or time allocation to the project.

Resources including Development and Quality Assurance are specifically trained to test for application security risks, and all committed code is peer reviewed and tracked to help ensure best practices are being followed.

Alongside monthly vulnerability scans and annual penetration tests, monthly static and dynamic analysis integrated into the build process further protects and validates system security.

BLUJAY APPLICATIONS

BluJay provides a range of supply chain and logistics management solutions with different functions and implementation/deployment options. Information on specific BluJay solutions is available separately. At a high level, all solutions include:

- Secure logon and user management
- Encrypted data in transit and at rest
- BluJay Change Management process
- Data Retention

Incident Response

BluJay has defined incident management policies and procedures to address security, confidentiality and privacy issues. As part of the Global Information Security Program, our Incident Management team employs industry-standard diagnostic procedures to drive resolution during business-impacting events. Operators provide 24x7x365 coverage to detect incidents and to manage the impact and resolution. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority.

We have implemented various methods of internal communication at a global level to help employees understand their individual roles and responsibilities and to communicate significant events in a timely manner. These methods include orientation and training programs for newly hired employees; regular management meetings for updates on business performance and other matters; and electronic ticketing systems to report such events.

BluJay also partners with our customers and third-party providers on various methods of external communication to support its customer base and the community. Mechanisms are in place to allow the customer support team to be notified of operational issues that impact the customer experience. Our internal business units and IT teams work together to provide transparent reporting and communication strategies to alert customers to any issues that may be of broad impact.

Additional Information

If you require further information, or have any questions please contact:

InfoSec@blujaysolutions.com

In Summary

At BluJay we take the security of our customers and protection of our and your data seriously. Customers using our service expect their data to be secure and confidential. Safeguarding this data is a critical responsibility we have, and we work hard to maintain that trust. The protection of user and internal data is a primary design consideration for all BluJay's infrastructure, applications, and personnel operations. We understand that data protection is more than just security; the purpose of this whitepaper is to provide our customers the assurance of the measures we take to uphold security in ALL areas.

BLUJAY
SOLUTIONS

BluJay Solutions helps companies around the world achieve excellence in logistics and trade compliance - it's in our DNA. Through a blend of Data, Networks, and Applications, delivered in the BluJay Way, our DNA platform powers the Frictionless Supply Chain for thousands of the world's leading manufacturers, retailers, distributors, freight forwarders, customs brokers, carriers, and logistics service providers.