Data Protection Policy

Purpose

This policy outlines the procedures and technical controls supporting data protection. [DCF-32, DCF-45]

Scope

Applicable production systems that create, receive, store, or transmit BluIP customer, personnel, or third-party data (hereafter "Production Systems") follow the requirements and guidelines described in this policy.

Policy

BluIP policy requires that:

- Data be handled and protected according to its classification requirements and be protected utilizing approved encryption standards, if applicable.
- Data of the same classification may be stored in a designated repository; production and lab data is segregated. Security controls, including authentication, authorization, data encryption, and auditing are applied according to the most restrictive classification of data in a repository.
- Personnel may not have direct administrative access to production data during normal business operations; exceptions may include emergency operations such as forensic analysis and manual disaster recovery.
- Services that are not necessary to achieve the business purpose or the function of the system may be disabled on all Production Systems.
- Access to Production Systems may be logged.
- Security monitoring, including activity and file integrity monitoring, vulnerability scanning, and/or malware detection, is enabled on Production Systems.
- Production systems undergo periodic scans for vulnerabilities. [DCF-18]
- Network segmentation and supporting documentation is maintained according to configuration standards outlined in the Asset Management Policy. [DCF-22]

Protection of Records

BluIP endeavors to shield its records from loss, destruction, falsification, and unauthorized access or release in alignment with legislative, regulatory, contractual, and business obligations.

Vendor Services

BluIP requests information from its providers about the security measures in place to protect records collected and stored providers related to BluIP's usage of their services

Data Protection Implementation and Processes

Customer Data Protection

BluIP hosts on cloud service providers in the **LAX** region by default. Data is replicated across multiple regions for redundancy and disaster recovery.

All BluIP employees adhere to the following processes to reduce the risk of compromising Production Data:

- implementation and/or review of controls designed to protect Production Data from improper alteration or destruction
- storage of confidential data in a manner that supports user access logs and automated monitoring for potential security incidents
- no modification of segmented Customer Production Data and access restricted to authorized Customers [DCF-61]
- production data at rest is stored on encrypted volumes using encryption keys managed by BluIP [DCF-54]
- protective security measures are employed in respect of volume encryption keys and machines that generate them; access controls are employed endeavoring to protect key material such that it is accessible only to privileged accounts [DCF-93]

Associated controls: DCF-1

Confidentiality/Non-Disclosure Agreement (NDA)

BluIP uses non-disclosure agreements to protect confidential information with legally enforceable terms applicable to both internal and external parties.

Customer Data Segregation Guidelines

Customer data is segregated using the following approaches.

- Logical Separation at Database/Datastore Level:
    - Customer is logically separated using a unique identifier for each customer.
    - At the API layer, customers authenticate with their chosen account, and the customer's unique identifier is included in the access token.
    - All database/datastore queries include the account identifier to restrict data access to the authenticated account.

- Dedicated Resources Allocation:
    - Alternatively, dedicated resources (database, computer) are allocated to each customer.
    - No customer may impact or access data or resources belonging to other customers.

AIVA®-Specific Data Segregation Mechanisms

AIVA employs specific mechanisms to ensure robust segregation of customer data

- Multi-Tenancy Architecture:
    - AIVA operates on a multi-tenancy architecture; each customer has their own isolated environment.
    - Data from different customers is logically separated and stored in dedicated resources

- Isolated Storage:
    - Customer data, including agent architectures and session information, is stored in isolated databases or data partitions.
    - Partitions are strictly segregated at the database level to prevent unauthorized access between customers.

- Scoped Access Control:
    - AIVA implements rigorous access control mechanisms; each customer account is associated with specific roles and permissions.
    - Access to data, configurations, and functionalities are governed within the application and API.
    - Users are authorized on a per-Customer basis, restricting access to its respective tenant only.

- Encryption for Data Protection:
    - AIVA uses industry-standard encryption algorithms to protect customer data both in transit and at

rest.
    - Encrypted data remains secure and less accessible to unauthorized parties during transmission and storage.

By adhering to these guidelines, AIVA better protects the integrity, confidentiality, and availability of customer data while maintaining employed separation between different customer environments.

Data Leakage Prevention

Data leakage prevention mechanisms are in place for systems that process, store or transmit sensitive information. These mechanisms are through email and other messaging technologies and generate audit logs and alerts. [DCF-150]

Additionally, incorporate data minimization, user consent and control principles along with encryption, access control, secure infrastructure, audit logging and alerts.

Access

BluIP Personnel access to production is subject to job position and is by default disabled. Temporary access may be granted after approval and review by the Engineering team on a case-by-case basis.

Role-based security is implemented for both internal and external users, with single sign-on (SSO) available for authentication into applications. Multi-factor authentication (MFA) is optional for external users and mandatory for Personnel, where technically possible or feasible. [DCF-58, DCF-59]

Monitoring

BluIP uses **AWS Cloud Watch®**[1]**, Azure Monitor®**[2] and other tools to monitor cloud service operations. Key personnel are notified via text, chat, and/or email in case of system failures or alarms. [DCF-81, DCF-189]

BluIP systems that handle confidential information, accept network connections, or make access control decisions may record and retain audit logs sufficient to answer key questions in accordance with the Logging and Monitoring Policy. [DCF-177]

Associated controls: DCF:78, DCF:78, DCF:80

Data At Rest

Encryption

- Databases, data stores, and file systems are encrypted to the extent provided according to BluIP's Encryption Policy.
- Removable media devices (USB, external hard drives) and company-issued laptop hard disks are encrypted. [DCF-52, DCF-149]

Associated control: DCF-381.

Retention

Stored data is categorized, and a retention schedule applied in accordance with the Asset Management Policy, Data Classification Policy and Data Retention Policy. Considerations for retention timeframe include:

- statutory, regulatory or contractual requirements
- type of data (e.g., accounting records, database records, audit logs)

- type of storage media (e.g., paper, hard drive, server)

Associated control DCF-197.

Storage and Disposal

Stored data is stored and handled while at rest and ultimately disposed in accordance with the Asset Management Policy, Data Classification Policy, and Data Retention Policy. Considerations include:

- authorization to access or manage stored data
- identification of records and their retention period
- technology change and ability to access data throughout retention periods
- timeframe and format to retrieve data
- appropriate methods of disposal

Associated controls: DCF-107, DCF-108, DCF-109.

Data Deletion

Stored sensitive data that is no longer required is deleted, destroyed or returned to the owning party in accordance with contracts, BluIP's business objectives and applicable laws and regulations. A record of such deletion is kept.

- Subject to the owning party exercising a right to have sensitive data returned, when no longer needed or required to be retained for business or legal reasons,
    - hard-copy materials are destroyed to the extent they contain sensitive data. Destruction is performed through secure means (e.g., shredding, pulping, incinerating, etc.) so that the data cannot be readily reconstructed. Hard copy materials are stored in secure storage containers prior to destruction.
    - Electronic media with sensitive data is destroyed or rendered unrecoverable Data on hardware (e.g., hard drives) is disposed of through secure means, such as wiping or hard drive destruction.
    - Sensitive company or third party data in the cloud is disposed of using secure deletion methods provided by the cloud service provider, endeavoring to ensure that data is irrecoverably erased through cryptographic erasure techniques or overwriting mechanisms.

Associated controls: DCF-123, DCF-775

Data in Transit

Necessity

Data is transferred only where necessary for business processes or to satisfy legal requirements.

Transfer Factors

Before choosing the method of data transfer, the following factors are considered:

- nature, sensitivity, confidentiality, and value of the information
- size of data being transferred
- impact of loss during transit

Encryption

To protect the safety of data in transit:

- external data transmission may be encrypted end-to-end. This includes via cloud infrastructure and third-party vendors and applications.
- internet and intranet connections may be encrypted and authenticated using protective protocols, key

exchanges, and ciphers. [DCF-3, DCF-55]

Information Exchange

Information may be exchanged between BluIP's system and other systems as authorized under relevant agreement(s). These agreements cover security and privacy requirements, controls, and responsibilities for each system.

BluIP's agreements are reviewed and updated as needed.

End-user Messaging Channels

- Restricted and sensitive data is only transmitted over electronic end-user messaging channels with end-to-end encryption enabled.
- Messages are protected from unauthorized access, modification, or denial of service, in accordance with BluIP's classification scheme.
- Relevant legal requirements are followed.
- BluIP retains the right to approve and authorize the use of external public services, such as instant messaging, social networking, or file sharing.
- Stronger authentication will be implemented for publicly accessible networks than for private networks

Data De-identification/Masking

- De-identification or masking of sensitive data is employed according to the Data Classification Policy.
- Sensitive data de-identification is achieved through erasure or expungement, and thorough verification.

Activity Review

System activities undergo regular review, occurring at intervals no longer than a year and sooner as needed. Reviews include individual or combined assessments of:

- audit Logs
- access Reports
- Security Incident Tracking Reports

Associated controls: DCF-527, DCF-536

Footnote

[1] AWS CloudWatch and all related marks are trademarks of Amazon.com, Inc. or its affiliates.

[2] Azure Monitor" is a registered trademark of the Microsoft group of companies.

Revision History

Version	Date	Editor	Approver	Description of Changes	Format
1	2-23-24	Nikolay Krastev			

2	10-1-124	Stephanie Meckler			