Data Classification Policy

Purpose

This policy provides guidance to Personnel and third parties regarding BluIP’s information labeling and handling practices. It emphasizes common-sense measures to protect sensitive or confidential information (e.g., Confidential Information should not be left unattended in conference rooms). [DCF-102]

Scope

This policy applies to all information owned, managed, controlled, or maintained by BluIP. Information covered in this policy includes information that is received, stored, processed, or transmitted via any means. It encompasses all forms of information, including electronic and hardcopy formats and any other form of information regardless of the media on which it resides.

Policy

Data Classification Scheme

Data classification categorizes data based on sensitivity levels and potential impacts to BluIP if disclosed, altered, or destroyed without authorization. Each data type falls into these classifications:

1. Confidential/Restricted Data

Definition:

- Highly sensitive information. Data requiring the highest level of protection, such as PHI and PII, protected by privacy regulations or confidentiality agreements.
- Data classified as Restricted or Confidential poses serious risks if disclosed or altered without authorization.
- Examples include data protected by state or federal privacy laws (e.g., PHI, PII) and data covered by confidentiality agreements.

Security controls for this data include:

- **Access Control:** Disclosure is limited to individuals with a legitimate need-to-know. Prior to receipt of such information, each recipient shall have executed an agreement protecting the confidentiality of such information. Explicit authorization from the Security Officer/General Counsel/Chief Compliance Officer may be required.
- **Protection Measures:** Must be safeguarded against loss, theft, unauthorized access, and disclosure.
- **Data Disposal:** Must be destroyed when no longer needed, in accordance with company policies.
- **Incident Response:** Requires specific methodologies and procedures for incident handling.

2. Internal Use Data

Definition:

Non-sensitive information. Data is classified as Internal Use when unauthorized disclosure or alteration could lead to moderate risks. This includes proprietary and ethical considerations.

Key requirements include:

- **Access Control:** Restricted to personnel with a legitimate need-to-know. Default classification for data not labeled as Restricted/Confidential or Public.
- **Security Controls:** Basic security measures should be applied.

3. Public Data

Definition:

- Freely shareable both internally and externally once information has been approved for public release.
- Data is classified as Public when unauthorized disclosure, alteration, or destruction would pose little to no risk to BluIP and its customers.

Key requirements include:

- **Access Control:** No restrictions on access or usage.
- **Security Controls:** Limited controls to prevent unauthorized alteration or destruction.

4. De-identified Data

BluIP de-identifies data to remove personal identifiers while using and sharing it. If any personally identifying information is present, it is not considered de-identified.

Assessing Classification Level and Labeling

The goal of information security is to protect the confidentiality, integrity, and availability of Corporate and Customer Data. Each data classification reflects its potential impact on BluIP (refer to APPENDIX A for personal data categories related to privacy regulations).

If classification is unclear, refer to the following classification levels:

CLASSIFICATION LEVELS

CLASSIFICATION	POTENTIAL IMPACT OF LOSS
RESTRICTED • **Highly sensitive information** • Level of protection is dictated externally by legal and/or contractual requirements • Must be limited to only authorized employees, contractors, and business partners with a specific business need	**SERIOUS DAMAGE** would occur if Restricted information were to become available to unauthorized parties either internal or external to BluIP. Impact could include negatively affecting BluIP's competitive position, violating regulatory requirements, damaging the company's reputation, violating contractual requirements, and posing an identity theft risk.
CONFIDENTIAL **Restricted (may also be referenced as "Confidential" amongst the BluIP policies)** • **Highly/Sensitive information** • Level of protection is dictated internally by BluIP as highly sensitive and restricted • Must be limited to only authorized employees, contractors, and business partners with a specific business need	**SERIOUS/SIGNIFICANT DAMAGE** would occur if Confidential information were to become available to unauthorized parties either internal or external to BluIP. Impact could include negatively affecting BluIP's competitive position, damaging the company's reputation, violating contractual requirements, and exposing geographic location of individuals.
INTERNAL USE • **Non-sensitive Information** • Originating within or owned by BluIP, or entrusted to it by others. • May be shared with authorized employees, contractors, and business partners who have a business need, but may not be released to the general public, due to the negative impact it might have on the company's business interests	**MODERATE DAMAGE** would occur if Internal Use information were to become available to unauthorized parties either internal or external to BluIP. Impact could include damaging the company's reputation and violating contractual requirements.
PUBLIC • Information that has been approved for release to the general public • **Freely shareable** both internally and externally	**NO DAMAGE** would occur if Public information were to become available to parties either internal or external to BluIP. Impact would not be damaging or a risk to business operations.

Definitions

Data Type Definitions

- **Restricted Data:** General terms referring to data classified as Sensitive or Private according to this policy's classification scheme.
- **Internal Data:** All data owned or licensed by BluIP.
- **Public Information:** Information available in the public domain that was rightfully obtained by a third party without confidentiality obligations.

APPENDIX A

HANDLING CONTROLS PER DATA CLASSIFICATION

Handling Controls	Restricted	Restricted/Confidential	Internal Use	Public
Non-Disclosure Agreement (NDA)	Required	Required	May be Required	Not Required
Internal Network Transmission (wired & wireless)	• Encryption Required • Instant Messaging Prohibited • FTP Prohibited	• Encryption Required • Instant Messaging Prohibited • FTP Prohibited	• Encryption Required	• No Requirements
Labeling				
External Network Transmission (wired & wireless)	• Encryption Required • Instant Messaging Prohibited • FTP Prohibited • Remote Access Controls (VPN & MFA)	• Encryption Required • Instant Messaging Prohibited • FTP Prohibited	• Encryption Recommended • Instant Messaging Prohibited • FTP Prohibited	• No Requirements
Labeling				
Data at Rest (file servers, databases, archives, etc.)	• Encryption Required • Access Controls Required (Limit Unauthorized Use)	• Encryption Required • Access Controls Required (Limit Unauthorized Use)	• Encryption Recommended • Access Controls Required (Limit Unauthorized Use)	• Access Controls Required (Limit Unauthorized Use)
Labeling				
Mobile Devices (iPhone, iPad, USB Drive, etc.)	• Encryption Required • Remote Wipe, if possible	• Encryption Required • Remote Wipe, if possible	• Encryption Recommended • Remote Wipe, if possible	• No Requirements
Labeling				
Email (with and without attachments)	• Encryption Required • Do Not Forward	• Encryption Required • Do not Forward	• Encryption Recommended • Do Not Forward	• No Requirements

Handling Controls	**Restricted**	**Restricted/Confidential**	**Internal Use**	**Public**
Labeling				
Physical Mail	• Mark "Open by Addressee Only" • Use "Certified Mail" courier or other service where receipt is evidence	• Mark "Open by Addressee Only" • Use "Certified Mail" courier or other service where receipt is evidence	• Interoffice Mail or Public Delivery	• No Requirements
Labeling				

APPENDIX B

Privacy Regulation Key Terminology

GDPR	
Controller	The entity determining the purposes and means of processing personal data.
Processor	The entity processing personal data on behalf of the controller.
Processing	Any operation performed on personal data, including collection, storage, and disclosure.
Pseudonymisation	Processing that makes personal data no longer attributable to a specific subject without additional information.
Third Party	Any entity other than the data subject, controller, or processor authorized to process personal data.
Consent	A clear indication of the data subject's agreement to the processing of their personal data.
Personal Data Breach	A security incident leading to unauthorized access to personal data.

Revision History

Version	Date	Editor	Approver	Description of Changes	Format
1	2-22-24	Nikolay Krastev			
2	11-11-24	Stephanie Meckler, Mark Horton			