BairesDev Data Classification and Protection Standard

Data Classification and Protection Standard

Important

BairesDev complies with the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union to the United States. BairesDev has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/.

In compliance with the **Privacy Shield Principles**, BairesDev commits to resolve complaints about our collection or use of your personal information. EU individuals with inquiries or complaints regarding our Privacy Shield policy should first contact BairesDev at:

- **e-mail**: hr.support@bairesdev.com
- **Phone**: *US*: +1 408 915 4135 - *AR*: +54 11 5353 9840

BairesDev has further committed to cooperate with the panel established by the EU data protection authorities (DPAs) with regard to unresolved Privacy Shield complaints concerning human resources data transferred from the EU in the context of the employment relationship.

1 Introduction

1.1 Purpose

The Data Classification and Protection Standard defines the different classification levels that are used by the Company. The subsequent sections detail the security measures required for each of the classification levels.

The purpose of the Data Classification and Protection Standard is to provide additional detailed information necessary to comply with Data Management Standards. While this document provides a list of security controls for each of the classification levels, it is not meant to suggest that the list is complete and fully comprehensive. The categories listed are the most common ones that users will encounter during the process of information handling.

The standard includes the minimum requirements. It is acceptable to implement measures that are more stringent than what is documented in the standard or to fulfill contractual obligations with a client. Exceeding the minimum requirements does not necessitate a security exception. Security exceptions should only be requested if less stringent controls than the minimum recommended controls will be used.

1.2 Scope

This standard applies to all people working for or on behalf of the Company, whether Company employees or not, requiring access to any Company, client or other third-party data, systems or services. This includes all personnel affiliated with subcontractors and third parties, and all contract, vendor, part-time temporary and intern personnel, whether work is conducted at a Company or client location, either onsite or remotely.

1.2.1 Company Data

This standard applies to all Company data. Company data is defined as data originated by the Company or third parties which is controlled and used by the Company for the Company's business purposes, but excluding client data. This includes without limitation Personal Data of Company employees, job candidates, client, business and supplier contacts, website users and data about the Company, clients, suppliers, competitors, alliance and other business partners.

1.2.2 Client Data

If a client provides their own classification and protection standard then Company engagement teams should follow the more stringent standard in order to satisfy Client Data Protection (CDP) control objectives. Client engagement teams should use this standard as guidance to review and recommend the implementation of control objectives and, where necessary, ensure that any residual risk is appropriately accepted by both the Company and client.

Client data is defined as Business Data, Intellectual Property and Personal Data that is owned and/or controlled by clients of the Company. Client data does not include Personal Data relating to client personnel that the Company collects, controls and uses in the course of maintaining a business relationship with the client and for marketing purposes.

1.3 Types of Information

Information is the output of processing, manipulating and organizing data in such a way that it contains meaning or has value. Information may be stored and handled in different ways, and may have varying lifespans:

- Information Repositories (central storage of master versions of production information):
    - Data residing in centrally hosted Information Repositories is typically subject to all classification and protection controls.
    - Examples of Information Repositories include centrally hosted applications, SharePoint sites and other document repositories.
    - A Data Governor is accountable for the Information Repository.
- Transient Documents and Information (sensitive information not held within an Information Repository):
    - Some data classification and protection controls may not apply.
    - Examples of Transient Documents include documents in a draft format, perhaps being shared for review, and expected to be stored in an information repository when completed. Other examples include local copies of data where the master version is stored in an Information Repository.
    - Examples of other Transient Information include discussion and decision support documents, supporting materials for meetings, emails, ad-hoc data models; these are not related to Information Repositories.
    - Transient Documents and Information are typically stored on a local workstation or in email systems and therefore access is limited only to people with access to that workstation or email account.

2 Classification

2.1 Overview

Data must be identified and classified to ensure that Company data receives the appropriate level of protection. All Data Governors of Company data or client data must assess their data and apply appropriate protections based on data sensitivity and criticality.

- **Restricted** – Restricted data is highly sensitive, strategic data considered "Material, Non-Public" for which an investor would very likely consider important in deciding whether to buy or sell securities and that could affect the price of the security or other similarly sensitive data. By design, very few people have access to Restricted Information because its distribution is limited to only select individuals on a need-to-know basis.
- **Highly Confidential** – Highly Confidential data is sensitive data that can be distributed **only** to those individuals or groups within BairesDev and external parties* who need to know the information to do their jobs.
- **Confidential** – Confidential data is sensitive and must not be shared outside of BairesDev (and external parties where there is a need to know). In some cases, Confidential data can be shared broadly across BairesDev, but it should be shared only as necessary. All non-public information that is not classified as Highly Confidential or Restricted pursuant to this standard must be classified as Confidential.

- **Unrestricted** – Unrestricted data is not sensitive, and is data that is intended to be generally available to the public.

"External parties" may include suppliers and clients subject to non-disclosure agreements, or to others as required by law or court order.

2.2 Unrestricted Examples

Examples of Unrestricted data include but are not limited to, the following:

- BairesDev Company advertising literature once it has been published;
- Data contained on BairesDev's public website: {+}http://www.bairesdev.com+.

2.3 Confidential Examples

Examples of Confidential data may include, but are not limited to, the following:

- All Employee webcasts;
- BairesDev policies;
- Internal presentation materials, such as presentations about the BairesDev career model;
- Personal Data that is intended to be made widely available, including:
    - Employee phone or voice mail directory;
    - Information (including photos) posted by individuals at their BairesDev People Page;
    - Organization charts.

All Personal Data is considered either "Confidential" or "Highly Confidential." Personal Data includes any data associated with an individual who is reasonably identifiable from the data set.

2.4 Highly Confidential Examples

Examples of "Highly Confidential" data include, but are not limited to, the following:

- Alliance, client and supplier information that could cause financial, competitive, or reputational damage if made public (examples include customer lists, business plans and strategies);
- Non-public client-owned information or work products (e.g., system development deliverables);
- Business critical information regarding the Company's technology infrastructure, network security architecture, support systems, or facilities management (e.g., architecture/infrastructure designs, server configurations, network maps, and disaster recovery plans); or
- Passwords and configuration files for infrastructure components supporting applications;

- Most Personal Data of Company employees, job candidates, business and client contacts, or of the Company's clients' customers and employees, including, but not limited to:
    - Benefits, employee earnings, payroll information;
    - Information contained in pre-employment background checks;
    - Performance feedback forms;
- All Personal Data regulated by privacy laws, or in relation to which disclosure or misuse could lead to identity theft or other harm to individuals. Examples include:
    - Information that enables identity theft (e.g., name associated with one or more of the following: date of birth, national identifiers/SSN, passport, driver's license number);
    - Financial information (e.g., bank accounts, credit cards);
    - Health information;
    - Sensitive Personal Data (e.g., race, ethnicity, marital status, religion, political affiliations, membership of trade unions, sexual orientation or information on alleged or committed criminal convictions) or highly regulated data which varies by jurisdiction (e.g., phone records, investigative reports, information about minors);
    - Compilations of Personal Data/lists (e.g., large volumes of names associated with addresses, telephones numbers, email, date of births, hobbies etc.);
    - Real-time geo-location data.

2.5 Restricted Examples

Examples of Restricted data include, but are not limited to, the following:

- Financial statements and performance reports (including profit and loss, revenues reported, etc.);
- Financial forecasting and planning information;
- Earnings estimates, or changes in previously released estimates;
- Major litigation Information;
- Significant information on acquisition, merger or divestiture proposal or agreements;
- Changes in dividends or plans for a stock split;
- Gain or loss of a significant client or contract;
- Other impending publicity or announcements, whether they are about the Company or others;
- Major management changes or developments;
- Material non-public views of financial data.

3 Summary of Classifications and Controls

Below is listed the minimum set of controls and how they apply across the classifications. The 'Transient Documents & Information' column gives an indication of whether this control applies to those types of information. Details of the controls can be found in subsequent sections.

Control	Unrestricted	Confidential	Highly Confidential	Restricted	Transient Documents & Information
Labelling of Information	None.	Information must be labelled with Classification.			Control applies.
Authentication	None.	Enterprise ID and Password (with multi-factor Authentication for ESO enabled applications).			Control applies (with variations*).
Access Control List	None.	Share in accordance with principle of least privilege.	Information accompanied by access control list of users/roles that can access the information.		Control applies (with variations*).
Access Control Review Frequency	None.	At least annually.	At least every six months.	At least every three months.	Control does not apply.
Protection of Email	None.	Use best judgement. For Highly Confidential Personal data, email must be encrypted.		For Restricted data, email must be encrypted.	Control applies.
Instant Messaging	None.	Use secure technology (Skype for Business).			Control applies.

Disposal of Electronic Information	Files/data must be removed via the system's "delete" or "remove" function.		Information securely wiped, or devices destroyed.		Control applies.
Paper Document Protection and Disposal	None.	Securely store, do not leave unattended, securely dispose.			Control applies.
Use of Client Deliverables or Data Outside the Context of the Engagement	None.	Confirm right to use, sanitize deliverables.			Control applies.
Location of Production Data	None.	Stored on Company servers and backed up.			Control applies (with variations*).
Use of Production Data in Testing	None.	Approval required.	Approval required and masking personal data.	Only late phase testing. Approval required and masking data.	Control does not apply.
Data Transmission	None.	Transmission in accordance with the Encryption standard			Control applies.
Transactional Data Integrity	None.			The ability to materially impact Restricted Data must be controlled.	Control applies.

4 Control Details

4.1 Labelling of Information

	Unrestricted	Confidential	Highly Confidential	Restricted
Information Repositories	None.	Physical Media and Information must be labelled with Classification[#].		All documents that are classified as Restricted must be marked as **Material, Non-Public – Not To Be Distributed Further**
Transient Documents and Information				

[#] Data Governors are responsible for ensuring that Information is labelled with its Classification. Recipients of unlabelled Information should treat it as Confidential, unless it is otherwise indicated to be Unrestricted.

4.2 Authentication

	Unrestricted	Confidential	Highly Confidential	Restricted
Information Repositories	None.	Access provided using Enterprise ID and password. Multi-factor authentication is required for authentication to ALL applications using Enterprise Sign-On (ESO).*		
Transient Documents and Information		Company-provided devices require authentication via Enterprise ID and password; mobile devices and tablets require passwords / passcodes that are difficult to guess (e.g. not "1234").		

*Outlook uses Windows Integrated Authentication rather than Enterprise Sign- On (ESO) and does not have multi-factor authentication.

4.3 Access Control List

	Unrestricted	Confidential	Highly Confidential	Restricted
Information Repositories	None.	Access control configured to restrict access. In some cases this might be set to 'everyone' in the organization.	Access control list required to control who can access the information.	
Transient Documents and Information		No access control list required.	If the information is to be shared, one of the following options should be applied: i) Use technical means (such as Permissions functionality) to limit distribution of the information. ii) Apply a label stating Highly Confidential. Not To Be Distributed Further Without Authorization of the Sender. or **Material, Non-Public – Not To Be Distributed Further** iii) Use an access control list or access control procedure which sets out the names and/or roles of people who are authorized to view and edit (i.e write and delete) this type of document.	

NOTE: Where information relates to Client data and Client Deliverables, then access is limited to personnel on that account, and with personnel supporting that account.

4.4 Access Control Review Frequency

	Unrestricted	Confidential	Highly Confidential	Restricted	

Information Repositories	None.	Access lists and rights within the application and supporting infrastructure components must be reviewed **at least annually**.	Access lists and rights within the application and supporting infrastructure components must be reviewed **every six months**.	Access lists and rights within the application and supporting infrastructure components must be reviewed **every three months**.	
Transient Documents and Information		No access control review required.			

4.5 Protection of Email

	Unrestricted	**Confidential**	**Highly Confidential**		**Restricted**	
Information Repositories	None.	Does not apply.				
Transient Documents and Information		Personnel should use their best judgment to determine the proper level of protection. Ensure the recipient(s) of the email have a business need to access the information. For Highly Confidential Personal data, email must be encrypted.		For Restricted data, email must be encrypted.		

4.6 Instant Messaging

	Unrestricted	**Confidential**	**Highly Confidential**	**Restricted**	

Information Repositories	None.	Information must not be communicated via text message or using instant messaging technology that is not secure. Note: You can assume that when using standard Company tools to transmit data within the organization and with federated organizations (e.g. Skype for Business), these systems transmit data in a secure way.			
Transient Documents and Information					

4.7 Disposal of Electronic Information

	Unrestricted	Confidential	Highly Confidential	Restricted	
Information Repositories	Files/data must be removed via the system's "delete" or "remove" function. When backup tapes containing Confidential Data are decommissioned, the tape must be cleaned via the system's "delete" or "remove" function.		Devices that are decommissioned or redeployed must be securely sanitized or disposed of (see Appendix 1 Data Sanitization or Masking). Data must only be deleted once backups are taken to comply with the information's retention period. When backup tapes are decommissioned, the tape must be securely wiped or fully destroyed.		

Transient Documents and Information					

4.8 Paper Document Protection and Disposal

	Unrestricted	**Confidential**	**Highly Confidential**	**Restricted**	
Information Repositories	None.	The following security measures are required for the protection and disposal of paper documents: · Securely store papers when not in use. · Documents must not be left unattended on printers, facsimile equipment, copiers, etc. · Documents must be retained for the prescribed retention period according to policies. · Securely dispose of documents when they have met or exceeded their retention period by shredding them or placing them in the locked containers provided for that purpose. · Documents must not be provided to unauthorized users.			
Transient Documents and Information					

4.9 Use of Client Deliverables or Data Outside the Context of the Account

	Unrestricted	**Confidential**	**Highly Confidential**	**Restricted**	

Information Repositories	None.	In certain circumstances, it may be allowable to use project deliverables or data outside the context of the original engagement. · Before doing so, you must first confirm you have a right to do so under the terms of the original engagement, and if in doubt, refer to the Client Data Protection (CDP) plan for the account, or contact the Account or Engagement IS Lead or your supervisor or legal. · Prior to reuse or upload to the Knowledge Exchange, you must sanitize the deliverables or other data to remove client names, personally identifiable information, and other sensitive information that is not required or allowable for reuse. Once such sanitization has occurred, such deliverables may be treated as Confidential.			
Transient Documents and Information					

4.10 Location of Production Data

	Unrestricted	Confidential	Highly Confidential	Restricted	

Information Repositories	None.	Information should be stored on Company approved servers*. This will allow for the information to be backed up on a regular basis. Master versions of electronic should not be stored on laptops, workstations, smartphones, tablets or removable electronic media, regardless of whether the device is Company owned or a personal device.			
Transient Documents and Information		Where it is necessary to store transient documents and other transient information on devices, the devices must be encrypted. Sensitive electronic data must not be stored on home computers.			

- See the[|https://hostingservicecatalog.accenture.com/]Hosting Services Catalog for an inventory of approved internal and third-party hosting services and guidance on how to select an appropriate service

4.11 Use of Production Data In Testing

	Test Phase	**Data Type**	**Unrestricted**	**Confidential**	**Highly Confidential**		
Information Repositories	EARLY PHASES (e.g. Dev., Product Test)	Business	No Limitation	Approval Required		Approval Required	Prohibited
		Personal	N/A	Approval Required		Approval and Data Masked*	N/A

	LATE PHASES (e.g. UAT, Data Migration Test)	Business	No Limitation	Approval Required		Approval Required	Approval and Data Masked where feasible
		Personal	N/A	Approval Required		Approval and Data Masked where feasible**	N/A
Transient Documents and Information			Control Does Not Apply.				

*Not reversible by team

- ideally not reversible by team
  Where approval is required this must come from the Data Governor for Company data or the Accountable BairesDev Leader with confirmation from the client for client data
  The test environment must be appropriately secured.
  Access must only be provided to selected testers. They should confirm that they do not have access to any production data (e.g. local copies whether masked or not).

4.12 Data Transmission

	Unrestricted	**Confidential**	**Highly Confidential**	**Restricted**	

Information Repositories	None.	Data transmitted between two endpoints on a network must be transmitted in accordance with the Encryption standard. Note: You can assume that when using standard Company tools to transmit data within the organization (e.g. Outlook and SharePoint), these systems transmit data in accordance with the Encryption standard.			
Transient Documents and Information					

4.13 Transactional Data Integrity

	Unrestricted	**Confidential**	**Highly Confidential**	**Restricted**

Information Repositories	None.			Creation of or changes to Restricted Data must be controlled using a combination of control techniques, at the discretion of the Data Governor. This includes the Data Governor identifying and documenting the transaction thresholds and having the necessary security controls in place that limit the user function based on the allowed transaction thresholds.*
Transient Documents and Information				

- For example, key financial systems must have the appropriate controls in place that secure access to the systems and also their functions.
  1. Transaction thresholds: cannot process transactions above a certain materiality threshold; approval required above a set threshold.
  2. Detective controls: periodic review of transactions above a certain threshold; periodic activity reviews.

5 Access to personal data

Every individual has the right to request access to their personal data stored in our company databases, request their information to not being used for any kind of contact, or be definitely deleted. Those requests can be made to HR via email at hr.support@bairesdev.com.

5.1 Investigation and arbitration

Regarding the Privacy Shield participation, BairesDev might be subject of investigations and enforcement powers of the US Federal Trade Commission (FTC) and/or the Department of transportation. For more information check the Privacy Shield website.

Every individual person has the possibility, under certain conditions, to invoke binding arbitration.

5.2 Third parties access

BairesDev doesn't share information with any third party. All the personal information is used for HR or Commercial purposes, and you can request access or deletion as is described in section 5.

5.3 Transfer and disclosure to third parties

BairesDev is responsible for the processing of personal information it receives, under the Privacy Shield Frameworks, or subsequently transfers to a third party acting as an agent on its behalf. BairesDev complies with the Privacy Shield Principles for all onward transfers of personal information from the EEA to the United States, including the onward transfer liability provisions.

If **BairesDev** needs or requires the information to be transferred to a third party, each individual will be previously notified. This notification will include information about who is the receipt of the personal data and why is this needed, except if it is under law enforcement by public authorities.

BairesDev will obtain assurances from the recipient that it will:

1. Use the Personal Data only to assist BairesDev in providing, maintaining or improving services.

2. Provide at least the same level of protection for Personal Data as is required by the Privacy Shield Principles
3. Notify BairesDev if the recipient is no longer able to provide the required protections. Upon notice, BairesDev will act promptly to stop and remediate unauthorized processing of Personal Data by a recipient.

In some cases, the employee signs a contract with clauses which may include details about how his information is used by BairesDev or any client.

5.4 Choice and limit

You have the right to choose (opt-out) whether your personal data is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by you.
If you wish to opt-out, all you need to do is contact us using the information in section 5 of this document or using any other options on our BairesDev WebSite .

Applicable law allows certain exceptions to your ability to opt-out, such as where we are parties to a contract that is still being performed, where law requires us to maintain information tow warranty claims, or otherwise. Where applicable law permits us to retain and continue to use such information and we do so, we will do so only to the extent permitted or required by law.

If you contact us to opt-out, we will explain the options available and comply with your request as required by the Principles and applicable law.