pandata

Information Security, Data Protection and Privacy Policy

Updated Jul, 2018

Policy

Context and overview

Key details

Policy prepared by:	Cal Al-Dhubaib, Partner
Reviewed by:	Arwood Security Consulting
Approved by Managing Partners on:	Jul 18, 2018
Next Review date:	Jan 30th, 2019

Introduction

Pandata requires access to Client Data to deliver Data science service.

These may include, customer information, operational logistics, business contacts, employees, or other Data critical to the client's operation.

This policy describes how this Data must be collected, handled and stored to meet the company's Data protection standards — and to comply with applicable laws.

This policy describes how Pandata protects all Data used and its systems.

Why this policy exists

This Data and Information security protection policy ensures Pandata

- Complies with applicable data protection laws and federal regulations
- Complies with client-specific Data policies and procedures
- Protects the rights of clients and partners
- Protects employees of Pandata
- Is open about how it stores and processes Client Data
- Protects its Information Technology Assets
- Protects itself from the risks of a Data breach

Definitions

Data: Data is raw, unorganized facts that need to be processed. Data can be something simple and seemingly random and useless until it is organized.

Client Data: Client Data is Data provided to Pandata by a client or customer of Pandata.

Policy Scope

This policy applies to all employees of Pandata, contractors, consultants, and official partners of Pandata. Generally, our policy refers to anyone we collaborate with or acts on our behalf and may need occasional access to Data as “Responsible Entities”.

This policy applies to all Data that the company handles or is in possession of, even if that information technically falls outside of applicable data protection laws, client requirements, and / or federal regulations.

This policy is a minimum level of protection. Data will be protected as defined by applicable laws federal regulations and/or Client Data management agreements.

This policy applies to all technology equipment owned by Pandata or used by Responsible Entities using non-owned devices to render services and governs Pandata’s use of Software as a Service (SaaS) and ‘cloud’ based Information Technology Resources, collectively called ‘Information Assets’.

Responsibilities

Responsible Entities must ensure Data is collected, stored and handled appropriately. Specifically, Data will not be

- Communicated informally
- Stored for more than a specified amount of time
- Transferred to organizations, states or countries that do not have adequate Data protection policies
- Distributed to any party other than the ones agreed upon by the Data’s owner (exempting legitimate requests from law enforcement authorities)

Responsible Entities must ensure Pandata’s Information Assets, for which they have responsibility, are protected appropriately.

The **Managing Partners** are ultimately responsible for

- Ensuring that Pandata meets its legal obligations.
- Reviewing all Data protection procedures and related policies, in line with an agreed schedule.
- Arranging Data protection training and advice for the people covered by this policy.
- Handling Data protection questions from staff and others covered by this policy.
- Dealing with requests from individuals to see the Data Pandata controls regarding them (also called ‘subject access requests’).
- Checking and approving any contracts or agreements with third parties that may handle the company’s Third-party, Confidential, and Restricted Data.

The **Data Protection Officer, is** responsible for

- Collecting written consent for all data processing.
- Responding to requests from companies on the right to withdraw consent.
- Ensuring all Information Assets used for storing Data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party Information Assets the company is considering using to store or process Data. For example, cloud computing services or storage.
- Responding and coordinating all activities in response to any discovered breaches.

Data Management and Mitigation

Data classification

When dealing with Data, Pandata classifies Data generally into the following categories

- **Public:** any Data publicly available.
- **Third-party:** Data acquired from 3rd party sources to enrich Client Data.
- **Confidential:** any non-publicly available Data that are provided by a client. Pandata internal business plans and practices.
- **Restricted:** Data that could directly result in direct or indirect harm to individuals or organizations such as personally identifiable, protected health information, or critical security and safety operations, and any Pandata trade secrets and Data Science research.

Compliance

When applicable, we adhere to data protection laws or federal regulations affecting **Client Data,** such as, but not limited to, Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR). This includes providing mandatory training and appropriate Data storage and access provisioning, at cost.

De-identification procedures

When dealing with **Restricted Data**, we will make every effort to de-identify any Data elements not critical to the requested Data science services. When Restricted Data elements are required, we will work with Clients to develop a two-way encryption for affected Data.

Disclosure Procedures

In certain circumstances, Data disclosure may be required by federal law or legal action. Under these circumstances, Pandata will be required to disclose requested Data as demanded. However, the **Data Protection Officer** will ensure the request is legitimate, seeking assistance from the **Managing Partners** and Pandata's legal advisers where necessary. Pandata will take reasonable action, when possible, to contest legal action such that Data disclosure is limited.

Staff Guidelines

These rules describe how and where Data should be safely stored and accessed. Questions about storing Data safely can be directed to the designated project manager or **Data Protection Officer**.

Pandata will provide training to all Responsible Entities handling Pandata Information Assets, Data classified as Third-Party, Confidential or Restricted to help them understand their responsibilities.

- Specialized training and certifications such as for HIPAA are required of and provided to appropriate Responsible Entities.
- Upon hiring, and at least annually, Responsible Entities' are provided Data handling and Information Security training.

Client Data

- **At all times, Responsible Entities must adhere to Client-specified Data protection procedures and policies.**
- Client Data must be classified as Confidential or Restricted and be handled according to appropriate guidelines.

Confidential Data

- The only people able to access Data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**.
- Responsible Entities should keep Data secure, by taking sensible precautions and following the guidelines below.
    - Using **strong passwords** and ensuring they are never shared.
    - Using , an enterprise password management system that generates, encrypts, and stores secure passwords.
    - Confidential Data **should not be disclosed** to unauthorized parties, either within the company or externally, including non-designated entities in employ of Client.
    - Employees **should request help** from the designated project manager or the **Data Protection Officer** if they are unsure about any aspect of Data protection.
    - Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of within 2 years, unless legally required otherwise.

Restricted Data

- **All guidelines from confidential Data.**
- Where possible, Responsible Entities should attempt to work with Restricted Client Data on Client-owned systems.
- In addition to strong passwords, **two-factor authentication must be used**.
- When access to Restricted Data is required, Responsible Entities can request it from the designated Project Manager.
- When working with Restricted Data, Responsible Entities should ensure **the screens of their computers are locked** when left unattended.
- Restricted Data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.
- Every effort must be made to de-identify compromising Data elements not critical to delivery of Data science services.
- Data must be **encrypted before being transferred electronically**. The designated project manager can explain how to transfer Data.

Data Storage

Questions about storing Data safely can be directed to Pandata's designated project manager or **Data Protection Officer**.

When Data is **stored electronically**, it must be protected from unauthorized access, accidental deletion and malicious hacking attempts

- Data should be **protected by strong passwords** that are changed at least quarterly and never shared between employees.
- Data should be encrypted when it is transmitted across the Internet.
- Restricted Data must be encrypted when stored.
- If Data is **stored on removable media** (such as a removable hard disk or USB stick), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers** and should only be uploaded to an **approved cloud computing service**.
- All servers and computers containing Data should be protected by **approved security software and a firewall**.

When Data is **stored on paper,** it should be kept in a secure place where unauthorized people cannot view it. These guidelines also apply to Data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper should be kept **in a locked drawer or filing cabinet**. Employees should make sure paper and printouts are **not left where unauthorized, for example on a printer, copier or fax machine.**
- Employees should make sure paper and printouts are **not left where unauthorized people could see them**, such as on a printer.
- **Data printouts should be** disposed of securely when no longer required.

Information Asset Protections

Information Assets should be protected according to their risk. The **Data Protection Officer** is responsible for assessing and assigning risk of Information Assets.

Information Assets should adhere to the following requirements

- The Systems must run anti-malware software.
- The Systems must only be used for approved business purposes.
- The Systems must be password protected, with the passwords stored appropriately.
- The Systems must store Data appropriately and following the **Data Storage** guidelines outlined previously.

Software as a Service (SaaS) and other cloud-based Data storage products are Information Assets. The **Data Protection Officer** is responsible for ensuring they are configured securely and vendors are aware of the guidelines. SaaS Information Assets should

- Be configured with appropriate security settings.
- Store Data appropriately following the **Data Storage** guidelines.
    - Data at rest is encrypted according to agreed-upon protocols
    - Data access is permitted to authorized personnel
    - Data is archived with proper security protocols
    - Data is retrievable with proper authorization
- Follow Client Data sharing agreements and be consistent with client expectations for Data handling.

Non-Pandata owned Bring Your Own Devices (BYOD) must

- Have a password/pin set to unlock device
- Have data/disk encryption enabled if supported by the device and not be 'rooted'
- Have data erasure performed remotely upon report of loss or theft of the device or termination of the relationship with Pandata if possible
- Be regularly patch or upgrading device as required
- Be turned over to Pandata if a legal need arises
- Have cost covered for data/roaming/costs associated with the device