Information Security Policy

Introduction

At its core Be Data Solutions is an Information Technology driven business. Therefore information technology and the handling of information is intrinsic to what Be Data does, both in terms of the products and services we provide to our customers and clients and in terms of the day to dayoperation of the business.

Purpose

The purpose of this Information Security Policy is to:

- Define the information security responsibilities of Be Data as a business and of its employees
- Define how Be Data's information security responsibilities are to be met
- Ensure that all employees understand their responsibilities with respect to information confidentiality and integrity
- Protect Be Data Solutions from liability or damage through accidental or malicious misuse of IT systems

Scope

This policy applies to all employees and contractors working for Be Data Solutions, the information systems used by the business and anyinformation systems implemented or managed by Be Data on behalf of their clients.

The nature of Be Data's business involves delivering services as well as creating and managing software platforms which handle C2 data. Thismeans Be Data must fulfil a number of contractual and legal obligations in storing, managing and processing that data.

The table below defines the services Be Data offers and the information security responsibilities relevant to that service.

Service	Description	Responsibilities
BEDATA_APPS platform product development	This is the ongoing product development of the BEDATA_APPS Identity andAccess management platform.	• Ensuring product features support relevant information security capabilities for B2C and B2B Identity and Access Management (such as password encryption, API endpoint access control, Admin UI access control). • Ensuring secure development practices and coding standards are followed. • Ensuring staff are trained in secure development practices and understand the relevant security standards and protocols required to develop the product.
BEDATA_APPS platform implementation	This is the provisioning, configuration and customisation of the BEDATA_APPS platformfor a specific client or client project.	• Ensuring that the client's implementation of the BEDATA_APPS platform does not introduce information security holes or increase the risk of a databreach. • Ensuring data is handled in a manner which does not compromise the confidentiality or integrity of the data during any migration tasks of C2 data undertaken. • Notifying the client of any data protection and information security risks which could be introduced due to architectural or implementation choices. • Providing guidance on the best practice security implementation of the BEDATA_APPS platform. Ensuring staff are trained in relevant security practices and secure handling of customer data.

BEDATA_APPS platform hosting and management	This is the ongoing hosting and management of a client's BEDATA_APPS platforminstance.	• Ensuring appropriate level of network security in order to prevent unauthorised or malicious damage to or loss of C2 data. • Ensuring monitoring of services is in place in order to detect availability issues and anomalies created by abnormal or suspicious behaviour. • Ensuring access to C1 services is limited to applications or individuals authorised to do so by the C1. • Ensuring that auditing of access, both to the API endpoints and Admin interfaces is in place. • Ensuring C2 data is backed up regularly. • Ensuring that C2 data is not retained for any longer than the C1 had requested it to be retained for. • Ensuring security updates are regularly applied to systems.
Be Data Audience platform implementation	This is the provisioning, configuration and customisation of the Be Data Audienceplatform for a specific client or client project.	• Ensuring that the client's implementation of the Audience platform does not introduce information security risks or increase the risk of a data breach. • Ensuring data is handled in a secure manner during any migration tasks of C2 data undertaken. • Notifying the client of any data protection and security risks which could be introduced due to architectural or implementation choices. • Providing guidance on the best practice security implementation of the BEDATA_APPS platform. • Ensuring staff are trained in relevant security practices and secure handling of customer data.
Be Data Audience platform hosting and management	This is the ongoing hosting and management of a client's Be Data Audienceplatform instance.	• Ensuring appropriate level of network security in order to prevent unauthorised or malicious damage to or loss of C2 data. • Ensuring monitoring of services is in place in order to detect availability issues and anomalies created by abnormal or suspicious behaviour. • Ensuring access to C1 services is limited to applications or individuals authorised to do so by the C1. • Ensuring that auditing of access, both to the API endpoints and Admin interfaces is in place. • Ensuring C2 data is backed up regularly. • Ensuring that C2 data is not retained for any longer than the C1 had requested it to be retained for. • Ensuring security updates are regularly applied to systems.

Definitions

Term	Description
C1	The customer using Be Data's services/platforms
C2	The end customer or user of the C1
BEDATA_APPS	The product name of Be Data's Identity and Access management platform

Information Security Principles

- Information handled by Be Data should be classified according to its required level of Confidentiality, Integrity and Availability in order toensure the appropriate procedures and controls are in place for handling that information.
- Access to information should be granted only to authorised users according to the security classification assigned to that information
- Employees should have clearly defined roles and responsibilities with respect to Information Security Policy
- Employees should be granted access to information according to the Principle of Least Privilege

Policy

Information Classification

Be Data handles wide range of sensitive information, from internal employee records and accounting information, to C2 data. The different levels of classification are listed in the table below:

Classification	Description
Confidential	The highest level of confidentiality for company information. Should be subject to the tightest access controls, this may include commercially sensitive information, payroll etc. Essentially any information that could cause harm or damage to the company or an individual if it was compromised.
Restricted	Lower in confidentiality than Confidential information, access to Restricted information is granted to a wider set of employees than confidential information. In addition the potential damage or harm to company or individual in the event of a compromise is lower than that of Confidential information.
Internal use	Information that can be freely distributed to all employees, yet still remains sensitive enough not to be shared publicly.
Public	Information that can be shares publicly by the client
C1 Confidential	Information which relates to a client or customer, which is commercially sensitive in nature (e.g. contractual information, information covered by an NDA with the client)
C1 Restricted	Information which relates to a client or customer, which is not confidential yet remains sensitive (e.g. a client's project plan, roadmap or company strategy)
C2 Confidential	Information which relates to end users or customers of a client, that is also highly sensitive (e.g. login credentials, sensitive personal information)
C2 Restricted	Information which relates to end users or customers of a client which is not deemed personally sensitive to the C2 user, but is commercially sensitive to the C1 (e.g. non PII data, user preferences)

The table below describes the types of information handled by Be Data along with their classification.

Client/Internal	Information type	Classification
Internal	Employee records	Confidential
Internal	Payroll	Confidential
Internal	Company Strategy documents	Restricted
Internal	Company operational documents	Internal use
Internal	Company marketing content	Public
Client	Client contract, commercial agreements, information covered by an NDA	C1 Confidential
Client	Project communications, project documentation	C1 Restricted
Client (BEDATA_APPS)	User/Customer Records stored in BEDATA_APPS Identity store	C2 Confidential
Client (BEDATA_APPS)	User preferences stored in BEDATA_APPS extended profile store	C2 Restricted
Client (BEDATA_APPS)	Access logs	C2 Restricted
Client (Audience Platform)	User/Customer records stored in Be Data Audience platform	C2 Confidential
Client (Audience Platform)	Aggregated User/Customer data stored in Be Data Audience platform	C2 Restricted
Client (Audience Platform)	Access logs	C2 Restricted

Governance

Review

This Information Policy will be reviewed under the following conditions:

- When changes are made to the services or products which Be Data provides
- When Be Data is commissioned to work within a new industry sector
- A change to the Data Protection Policy or data protection requirements occur
- When a new information security tool, technique or practice becomes available
- In response to a security incident or data breach

In the case of Be Data offering a new type of service or product, this will trigger a board level review of the offering which will encompass identifying any additional information security responsibilities Be Data will acquire as well as trigger the planning of relevant organisational changes, proceduresor practices.

- Once an organisational or procedural change is established, the Board will agree with the Information Security Manager the deadlines for implementation of the changes.

Implementation

The Information Security Manager will monitor progress of any changes required and notify the board in the event of insufficient progress.

Notification

This Information Security Policy will be published to Be Data's internal staff Confluence website.

New employees will be asked to read the policy and sign a statement confirming they have understood it.

Upon an update to the policy, a company wide email notifying employees of changes to Be Data's Information Security Policy will be sent, instructingemployees to read the updated policy.

Compliance

The Information Security Manager is responsible for ensuring regular audits of processes and procedures are undertaken to identify instances where compliance is not being met.

Where and employee fails to follow a company policy, this will be reported to their line manager to deal with. In situations where an employee repeatedly fails to follow company policy, the employees line manager will be asked to escalate the problem via disciplinary procedures.

Where the instance of non-compliance is wider than an individual employee's actions, or is a systemic issue, then this will be reported to the Board.