POLICY FOR PROVIDING DATA TO CLIENTS

Code:	
Version:	v 1.11
Date of version:	09/09/2024
Created by:	Casey Eldib, James Paul & Brad Unal
Approved by:	Metin Unal
Confidentiality level:	Confidential

CHANGE HISTORY

Date	Version	Created by	Description of change
24/04/2017	1.0		Basic document outline
28/04/2017	1.2	Brian Grant	Vormetric cryptographic key and control details added
02/05/2017	1.3	James Paul	Reviewed
18/07/2017	1.4	James Paul	Updated
18/07/2018	1.5	Fiona Nicholls	Reviewed/updated
03/09/2019	1.6	Di Parker	Reviewed/updated
13/09/2020	1.7	Mark Needham	Reviewed/updated
09/09/2021	1.8	Mark Needham	Reviewed/updated
07/09/2022	1.9	Mark Needham	Reviewed/updated
11/09/2023	1.10	Mark Needham	Reviewed/updated
09/09/2024	1.11	Mark Needham	Reviewed/updated

TABLE OF CONTENTS

1. Purpose

This policy outlines the procedure for downloading and sending client data upon request. It ensures that all data, including call data, captured information, and reporting, is handled in a secure, compliant, and efficient manner while adhering to Australian privacy laws and data protection standards.

2. Scope

This policy applies to all employees of the contact centre who are involved in handling, processing, and transferring client data, including customer service agents, supervisors, managers, and IT staff.

3. Types of Data Included

The client data covered under this policy includes, but is not limited to:

- **Call Data**: Recordings of calls and associated metadata (e.g., call time, date, duration).
- **Data Captured During Calls**: Any information collected during the call (e.g., personal details, service requests, feedback).
- **Reports**: Performance reports, customer interaction summaries, and data analytics related to the client's account.

4. Procedure for Client Data Requests

4.1. Client Request Submission

- Clients must submit a formal written request for their data, which may be done via email or an online request form.
- The request must include:
  - Client's full name
  - Account or reference number
  - Specific data being requested (e.g., call recordings, reports)
  - Preferred method of receiving the data (e.g., email, secure file transfer)

4.2. Request Validation

- The request will be reviewed by the **Customer Support Team** to validate the client's identity and ensure authorisation. This may include:
  - Verifying account details
  - Confirming the client’s identity through two-factor authentication (2FA) or other verification methods
- If the request is invalid or incomplete, the client will be contacted for clarification.

4.3. Authorisation and Approval

- Once validated, the request must be authorised by the **Contact Centre Manager** or **Compliance Officer** to ensure that it complies with privacy and data protection laws.
- Any data requested must be reviewed to ensure it is relevant, accurate, and necessary for the client's needs.

4.4. Data Preparation and Download

- **IT/Data Management Team** will handle the secure extraction and preparation of the requested data, ensuring:
  - Call recordings and associated metadata are included.
  - Any personal data captured during calls is formatted appropriately.
  - Reports are generated in the requested format (e.g., CSV, PDF).
- Data will be checked for accuracy and completeness by a second team member for quality assurance.

4.5. Data Transfer and Security

- Data will be delivered to the client using a secure method based on their preference, such as:
  - **Email**: Data can only be sent via email if it is encrypted and password protected, with password provided in a sperate manner.
  - **Secure File Transfer**: Large files or sensitive data will be shared through a secure file transfer protocol (SFTP) or a trusted cloud platform with password protection and expiration.
- Under no circumstances should sensitive data be sent via unencrypted channels.

4.6. Notification

- Once the data has been successfully sent, the client will be notified via email, confirming the transfer and providing any relevant instructions for accessing the data.

5. Data Retention Compliance

- A record of the data request, approval, and transfer must be documented in the **Client Data Request Log** and stored for audit purposes for 7 years in accordance with the company's data retention policy.
- All data transfers will comply with Australian Privacy Principles (APPs) under the **Privacy Act 1988** and any other relevant legislation.

6. Roles and Responsibility

- **Customer Support Team**: Validate the client request and ensure all required information is provided.
- **Contact Centre Manager/Compliance Officer**: Authorise the release of client data and ensure the process complies with legal requirements.
- **IT/Data Management Team**: Extract, prepare, and transfer the requested data securely.
- **Quality Assurance Team**: Double-check the accuracy and completeness of the data before it is sent.

7. Security and Privacy Considerations

- All employees must adhere to data protection guidelines to ensure client information is kept confidential and secure throughout the process.
- Client data will be encrypted both in transit and at rest, and access to the data will be restricted to authorised personnel only.

8. Breaches and Incidents

In the event of a data breach or improper handling of client information during the data request process, the incident must be reported immediately to the **Compliance Officer**. Affected clients will be notified in accordance with the company's Data Breach Response Plan.

9. Review and Amendments

This policy will be reviewed annually to ensure compliance with evolving legal requirements and internal procedures. Any amendments will be communicated to all employees.

10. Validity and document management

This document is valid as of 09/09/2024

The owner of this document is CTO, who must check and, if necessary, update the document at least once every six months.

Managing Director

Metin Unal