



Data Retention Policy

Version 1.1

October 2023

DOCUMENT METADATA

Document Author

Document Author(s)	Annsheila Gitungo
--------------------	-------------------

Change Record

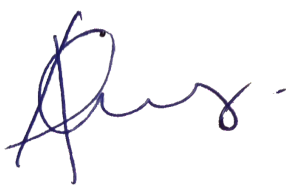
Issue Date	Version No	Status: (Current, Obsolete, Archived)	Comment/Reason
17 th April 2023	1.0	Obsolete	First Draft
17 th October 2023	1.0	Updates based on SISA Review	Updates based on Sisa Reveiw

Document Review

Date of Next Review	As the need arises/Annually
---------------------	-----------------------------

Approval

This document has been approved by the undersigned

Name	Role/Position	Signature	Date
Fredrick Mainga	Head of Tech		17/10/2023
Annsheila Gitungo	Head of Compliance & Risk		21/10/2023

Data Retention Policy for Lipad Tech Limited

Overview

This document outlines the data retention policy for Lipad Tech Limited to ensure that the company complies with all relevant laws and regulations regarding data retention. The policy applies to all data created, received, and maintained by the company, whether in paper or electronic form.

Data Storage Locations

The following shows applications and locations where card data is handled within the Lipad ecosystem as currently architected:

Category	Name	Assigned Hostname/IP	Type	Current DC	Location
Checkout	lipad-checkout-ui-prod	https://lipad-checkout-ui-prod-3zzyi.ondigitalocean.app/	App	BLR1	Bangalore, India
	lipad-checkout-api-prod	https://lipad-checkout-api-prod-wiuvp.ondigitalocean.app/	App	LON1	London, United Kingdom
Database	lipad-postgresql-prod-01	lipad-postgresql-prod-01-do-user-9659290-0.b.db.ondigitalocean.com	Database	LON1	London, United Kingdom

Policy

1. Purpose

The purpose of this Data Retention Policy is to ensure that Lipad Tech Limited (hereinafter referred to as "the Company") maintains the highest standards of data security and compliance with relevant regulations, particularly regarding cardholder data. This policy outlines the procedures for identifying and securely deleting stored cardholder data that exceeds the defined retention period.

2. Scope

This policy applies to all employees, contractors, and third-party service providers who have access to cardholder data within Lipad Tech Limited.

3. Definitions

- **Cardholder Data:** Any personally identifiable information associated with a cardholder. This includes primary account number (PAN), cardholder name, expiration date, and service code.
- **Retention Period:** The duration for which cardholder data is stored by the Company.

4. Data Retention Schedule

- The retention period for cardholder data is defined as [insert specific time frame, e.g., 90 days].
- Beyond this period, cardholder data should be promptly identified and securely deleted from all storage systems.

5. Quarterly Data Purge Process

To ensure compliance with the defined retention period, the Company will conduct a quarterly process for identifying and securely deleting stored cardholder data. This process will include the following steps:

5.1. Data Inventory

- Conduct a comprehensive inventory of all systems and databases that store cardholder data.
- Document the location, type, and volume of cardholder data stored in each system.

5.2. Data Assessment

- Review the data inventory to identify cardholder data that has exceeded the defined retention period.
- Cross-verify with transaction records and relevant logs to confirm the accuracy of the retention period.

5.3. Authorization and Documentation

- Obtain necessary authorization from the designated personnel for the deletion of identified cardholder data.
- Document the details of the authorization, including the date and the individuals involved.

5.4. Secure Deletion Process

- Utilize secure deletion methods to permanently remove cardholder data from storage systems.
- Confirm the successful deletion of data and maintain records of the deletion process.

5.5. Monitoring and Reporting

- Regularly monitor the success of the quarterly data purge process.
- Generate reports summarizing the deleted cardholder data, retention compliance, and any deviations.

6. Training and Awareness

Conduct regular training sessions for employees involved in the data purge process to ensure understanding of the policy and compliance requirements.

7. Non-Compliance Consequences

Failure to comply with this Data Retention Policy may result in disciplinary action, including but not limited to warnings, suspension, or termination of employment or contract.

8. Review and Revision

This Data Retention Policy will be reviewed annually and updated as needed to ensure continued compliance with regulations and industry best practices.

9. Contact Information

For questions or concerns regarding this policy, contact the [insert relevant department or individual].

Conclusion

Lipad Tech Limited's data retention policy aims to ensure that data is retained only as long as necessary, is destroyed securely, and is backed up regularly. All data will be classified based on its sensitivity, importance, and legal requirements to determine its retention period and destruction requirements. The policy will be communicated to all employees, contractors, and third-party vendors who handle company data, and compliance with legal and regulatory requirements will be ensured. Any exceptions to the policy must be approved by the company's legal and compliance team and documented appropriately.

Contact Us

If you have questions regarding our data retention policy or any enquiries, kindly contact us via the information below:

OPERATIONS
HEADQUARTERS
LIPAD TECH LIMITED
George Padmore Rd,
Nairobi Kenya
Email: info@lipad.io
Phone number: +254112495342