Data Retention , Retrieval and Secure Disposal Policy

Document Information

Organization Name	**LivQuik Technology (India) Private Limited**
Document Name	Data Retention , retrieval and Secure Disposal Policy
Latest Version No	**1.9**
Date	**03rd November 2021**
Authored By	**Vaibhav Singh**
Reviewed By	**Madhur Karnik**
Approved By	**Yudhajit Nag**

Version History

Ver. No.	Release Date	Change History	Authored / Revised By	Reviewed By	Approved By
1.0	01 Feb 2013	**New**	QA Lead	Module Lead	CTO
1.1	02-Aug-2014		QA Lead	Module Lead	Yudhajit Nag
1.2	04-Aug-2015		QA Lead	Module Lead	Yudhajit Nag
1.3	26-Jul-2016		QA Lead	Module Lead	Yudhajit Nag
1.4	07-Aug-2017		Vaibhav Singh	Madhur Karnik	Yudhajit Nag
1.5	07-Sep-2018		Vaibhav Singh	Madhur Karnik	Yudhajit Nag
1.6	12-Apr-2019		Vaibhav Singh	Madhur Karnik	Yudhajit Nag
1.7	08-Jun-2020		Vaibhav Singh	Madhur Karnik	Yudhajit Nag
1.8	12-Apr-2021		Vaibhav Singh	Madhur Karnik	Yudhajit Nag
1.9	03-Nov-2021	**Latest Version**	Vaibhav Singh	Madhur Karnik	Yudhajit Nag

1. Scope

This policy applies to all physical and electronic media assets of LivQuik

2. Policy

The entire LivQuik records, either physical or digital, are subject to the retention requirements based on business, legal and regulatory requirements. LivQuik requires that all removable storage media (CDs, tapes, memory sticks, hard drives, etc) are clean (which means: it is not possible to read or re-constitute the information that was stored on the device or document) prior to disposal. Specifically:

No storage of Magnetic stripe data, CVV, CID, CAV2, CVV2, CVC2 and PIN to be stored under any circumstances.

Each data item that is stored should be marked with the name of the record, the record type,the original owner of the data, the information classification, the required retention period, and any special information (eg in relation to cryptographic keys).

No Transactional/System Data is deleted from the system, case where user wants to "delete" his account we change inactive status as N and deleted flag as Y in the database enforcing application to skip this information. The records both physical and electronic should have secure remote offsite backups.

The offsite records both physical and digital should be retrieved and reviewed at least annually or based on the criticality of the information of the records.

All records (physical and digital) moving to and fro the facility to offsite locations has to be logged and inventory managed both at the primary and offsite locations. A periodic inventory check must be done at offsite to find if there exist any irregularities in the logging mechanism.

Data should be disposed as soon as the specified retention period completes it retention period.

If sensitive authentication data (CVV, PIN, magnetic stripe data, track data etc.) is being received, then the data should not be stored and be deleted in a secure manner which makes the data unrecoverable.

Cryptographic keys, which are required for sensitive transaction data should be retained as set out as in <Credit Card Data Encryption & Key Management Policy >

Devices containing confidential information are dependent on a risk assessment physically destroyed prior to disposal and are never to be re-used.

Devices containing confidential information that are damaged are subject to a risk assessment prior to sending for repair, to establish whether they should be repaired or replaced.

Documents, CDs, etc containing confidential and restricted information which are to be destroyed are shredded by their owners, using a cross cut shredder. These shredders are located in the secure area and the containers are under lock and key.

Portable or removable storage media of any description are physically destroyed prior to disposal.

The data owner along with support from the custodian is responsible for destroying data once it has reached the end of the retention period. Destruction must be completed within 30 days of the planned retention period. Destruction is handled as follows:

Papers to be shredded.
CDs to be shredded.
Backup tapes to be burnt.
Sensitive data to be deleted through a program.

The <Name the responsible area> is responsible for the retention and secure disposal of storage media and the disposal of all information processing equipment is routed through his office. A log <Documents Data Transfer and Storage Request Form_v1 & Data Disposal Form_v1> is retained showing what media were destroyed, disposed of, and when. As required, the asset inventory is adjusted once the asset has been disposed of.

The Nodal Officer is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above.

Data Breach Notification Policy

Document Information

Organization Name	**LivQuik Technology (India) Private Limited**
Document Name	**Data Breach Notification Policy**
Latest Version No	**1.9**
Date	**03rd November 2021**
Authored By	**Vaibhav Singh**
Reviewed By	**Madhur Karnik**
Approved By	**Yudhajit Nag**

Version History

Ver. No.	Release Date	Change History	Authored / Revised By	Reviewed By	Approved By
1.0	01 Feb 2013	**New**	QA Lead	Module Lead	CTO
1.1	02-Aug-2014		QA Lead	Module Lead	Yudhajit Nag
1.2	04-Aug-2015		QA Lead	Module Lead	Yudhajit Nag
1.3	26-Jul-2016		QA Lead	Module Lead	Yudhajit Nag
1.4	07-Aug-2017		Vaibhav Singh	Madhur Karnik	Yudhajit Nag
1.5	07-Sep-2018		Vaibhav Singh	Madhur Karnik	Yudhajit Nag
1.6	12-Apr-2019		Vaibhav Singh	Madhur Karnik	Yudhajit Nag
1.7	08-Jun-2020		Vaibhav Singh	Madhur Karnik	Yudhajit Nag
1.8	12-Apr-2021		Vaibhav Singh	Madhur Karnik	Yudhajit Nag
1.9	03-Nov-2021	**Latest Version**	Vaibhav Singh	Madhur Karnik	Yudhajit Nag

Data Breach Notification Policy

Purpose:

The purpose of this document is to define broad policy applicable to Notification of a Data Breach in the Company.

Any Information that is created and obtained during employee tenure at LivQuik India pvt ltd comes under the scope of DLP. which is further elaborated as:

1 Any employee, contractor or individual with access to systems or data.

2 Definition of data to be protected

· Personally identifiable information- any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.

Financial – consists of pieces or sets of information related to the financial health of a business. The pieces of data are used by internal management to analyze business performance and determine whether tactics and strategies must be altered.

· Restricted/Sensitive – Non-public Information is defined as any information that is classified as Private or Restricted Information according to the data classification scheme defined in this Guideline. Sensitive Data is a generalized term that typically represents data classified as Restricted, according to the data classification scheme defined in this Guideline. This term is often used interchangeably with confidential data.

· Confidential – Data should be classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the companies or its affiliates. Examples of Restricted data include data protected by state or federal privacy regulations and data protected by confidentiality agreements. The highest level of security controls should be applied to Restricted data.

Private – Data should be classified as Private when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the companies or its affiliates. By default, all Institutional Data that is not explicitly classified as Restricted or Public data should be treated as Private data. A reasonable level of security controls should be applied to Private data.

Public – Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would results in little or no risk to the companies and its affiliates. Examples of Public data include press releases, course information and research publications. While little or no controls are required to protect the

confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.

EMPLOYEE AGREEMENT

Employee NDA is signed by the employee at the time on joining the companies which highlights keys policies that are undertaken to prevent any data leakages during and after the tenure of the employee. Any leakages of Critical information by the employee during and after his tenure will have legal consequences which is governed by the NDA document.

Data Breach:

"Data Breach" for the purpose of this policy means any disclosure of data not authorized under the "Data Access" or "Data Disclosure" policies of the Company.

Exceptions:

a) When data is unauthorizedly accessed by an employee of the organization who is not normally authorized to access the data.
b) When data is demanded by a law enforcement agency under any valid provision of law and furnished in compliance of such demands.
c) When data is “Potentially accessible” by an unauthorized person because of an identified vulnerability, but there is no clear indication of such access as revealed by an internal investigation at the level of the Compliance official.
d) When data is handed over to a third party based on a valid authorization and in terms of the contractual obligations between the Company and the third party.
e) When the data which is suspected to have been breached is **not** associated with personal identification,
f) When the data which is suspected to have been breached is “Encrypted” and the decryption key associated with the encrypted data is not also suspected to have been breached to the same attack source.
g) When the data which is suspected to have been breached is already in the public domain.

First Response

The identification of an incident as a “Potential Data Breach Incident” may be made by any person within or outside the company and as soon as it comes to the knowledge of any of the employee of the organization, it shall be his duty to report to the Compliance Official for further action.

Whenever an incident is flagged as a “Potential Data Breach Incident”, the Compliance official shall raise an Incident ticket.

As a first response, the Compliance official shall immediately conduct a preliminary internal investigation to identify the impact of the suspected data breach and determine whether a data breach notification is required under this policy.

The report shall then be sent to the WTD for further action.

External Investigation

Where necessary, the internal investigation team may refer the matter to a specialized external agency to investigate and determine the nature of the suspected breach and its impact before further action is initiated under this policy.

Examination of Investigation Reports

The reports of the internal team and the external team where available shall be submitted for further action to the WTD. WTD shall seek the recommendations of the ISCGC to decide if a data breach notification is required and if so the details of such notification.

Issue of Data Breach Notification Release

The WTD after considering the opinion of the ISCGC will issue a "Data Breach Notification Release" to the Compliance Officer indicating the action to be taken which should include instructions as to whom the notification is required to be given, when and with what information.

Evidence Preservation

In all suspected data breach investigation, irrespective of the final outcome of the investigation, all evidence collected during the investigation is preserved and archived in a legally acceptable format so as to be retrievable when necessary with appropriate authentication.

Data Beach Notification Release

Whenever the incident is confirmed to have resulted in the breach of data as defined in the policy, following actions shall be taken within 30 days from the confirmation of the data breach.

1. All individuals, whose data has been directly collected by the representative of the company and where there is a breach, the employee has a right to be terminated without notice.

Sanctions

Where the investigation has found the involvement of negligence of any of the employee/s and non-compliance of information security policy of the organization, the

Company shall initiate necessary action as per the **Sanction Policy** adopted by the organization.

Police Complaint

Where the data breach incident has been caused by a deliberate act of either an employee or an outsider, a formal complaint can be lodged with the local Police authorities .

Data Disclosure Policy

Document Information

Organization Name	**LivQuik Technology (India) Private Limited**
Document Name	**Data Disclosure Policy**
Latest Version No	**1.0**
Date	**03rd November 2021**
Authored By	**Vaibhav Singh**
Reviewed By	**Madhur Karnik**
Approved By	**Yudhajit Nag**

Version History

Ver. No.	Release Date	Change History	Authored / Revised By	Reviewed By	Approved By
1.0	03 Nov 2021	New	Vaibhav Singh	Madhur Karnik	Yudhajit Nag

Data Disclosure Policy

Purpose:

The purpose of this document is to define broad policy applicable to disclosure of data in the hands of the Company.

"Disclosure" in respect of any "Data", means allowing access or transmitting information by the organization to any person who is not otherwise permitted access to the said data as per the "Access Policy" of the Company read along with the "Data Classification Policy."

Policy

Data Disclosure request may emanate from inside the organization or from outside. When data is requested from outside, the request will be routed through the Compliance Official who will be considered as the originator of the request for further processing of disclosure within the organization.

No custodian of data shall disclose the data to any person without authenticated permission from his team leader. It shall be the responsibility of the custodian to seek, obtain and preserve authorization of his team leader for disclosing any data.

Any person who generates a "Disclosure Request" shall send the request to his team leader who in turn forwards it to the leader of the team of the custodian of the data.

"Disclosure request" shall properly describe the data required, the purpose, the duration up to which such data is required and any other information relevant for the disclosure.

It shall be the responsibility of the "Data Requisitioned" to strictly adhere to the terms of disclosure including the period after which the data may be required to be destroyed.

During the time data is shared under a disclosure request, the receiver shall be considered as the Co-Custodian of the data and shall be responsible for its custody as per the data classification policy and access policies.

A "Data Movement Register" shall record all disclosures and the "Data Movement Ticket" shall not be closed until the moved data is destroyed.

A detailed procedure for handling the "Data Disclosure" shall be developed.

Whenever a data disclosure request is received from an external agency such as a law enforcement agency, it shall be the responsibility of the Compliance Official to verify the authenticity of the request before forwarding the request for further processing. He shall however ensure that there is no undue delay in responding to such disclosure request.

When a disclosure request is received from the Law enforcement authorities, the request shall be acknowledged within 24 hours. Where the request is not authenticated either with the use of a digital signature or a trusted source verification, a counter request shall be sent for an authenticated message.

All disclosures of data to external parties shall be accompanied by a certificate as required under Section 65B of Indian Evidence Act by the person responsible for the data disclosure.

Where the disclosure request requires emergent response without verification of the authenticity of the person requesting the data, the Compliance officer shall immediately contact the WTD and act under his directions.

Document Information

Organization Name	**LivQuik Technology (India) Private Limited**
Document Name	**Access Policy**
Latest Version No	**1.9**
Date	**03rd November 2021**
Authored By	**Vaibhav Singh**
Reviewed By	**Madhur Karnik**
Approved By	**Yudhajit Nag**

Version History

Ver. No.	Release Date	Change History	Authored / Revised By	Reviewed By	Approved By
1.0	01 Feb 2013	New	QA Lead	Module Lead	CTO
1.1	01-Feb-2014		QA Lead	Module Lead	Yudhajit Nag
1.2	03-Feb-2015		QA Lead	Module Lead	Yudhajit Nag
1.3	03-Feb-2016		QA Lead	Module Lead	Yudhajit Nag
1.4	16-Aug-2017		Vaibhav Singh	Madhur Karnik	Yudhajit Nag
1.5	24-Sep-2018		Vaibhav Singh	Madhur Karnik	Yudhajit Nag
1.6	10-Apr-2019		Vaibhav Singh	Madhur Karnik	Yudhajit Nag
1.7	06-May2020		Vaibhav Singh	Madhur Karnik	Yudhajit Nag
1.8	02-Mar-2021		Vaibhav Singh	Madhur Karnik	Yudhajit Nag
1.9	03-Nov-2021		Vaibhav Singh	Madhur Karnik	Yudhajit Nag

Access Policy

Purpose:

The purpose of this policy is to define the policy for personal and Sensitive personal information of individuals that are processed by the Company.

Policy

The essence of the Access policy is that

a) Data in the hands of the Company whether in storage, processing or transmission is classified as per the Data Classification Policy with an appropriate security tag.
b) Data Access is provided strictly on a "Need To Know" basis.
c) Data is tagged with a "Custodian" who is the owner of the data and is ultimately responsible for the data to be accessed as per the policy.

How Access is Granted

Request for access to any data is generated from the Team Leader on request by the user or otherwise as per requirement of a project along with the required privileges by the team leader of the user team.

The permission to access when granted is tagged with the period for which the permission is granted.

The employee ID is created by the HR department at the time of joining and used for creation of access credentials.

How Access is Withdrawn

Access to data is withdrawn based on the terms on which the access was initially granted.

Access may also be withdrawn based on the request for such withdrawal.

Such "Access Withdrawal Request" shall be sent by the person who originates the request to his team leader who in turn sends it to the technical team that is resposnible for maintenance of the access.

The technical team shall take the necessary action to withdraw the access under information to other Co-Custodians.

Before any employee is relieved from his duties on acount of termination or transfer to alternate responsibilities, The leader of the team of the outgoing employee shall provide clearance to the HR department in this regard before the relieving order is confirmed. All company owned assets will be taken back by the HR and the same information is passed on to the Admin Head for updation of data in inventory register .

A separate Password policy explained below provides the guideline to the employees for setting the Password for access of data.

The Organization has standard user access profiles – only **Yudhajit Nag** (CTO), **Vaibhav Singh** (QA Lead), **Madhur Karnik** (Module Lead) are authorized to access production systems using two-factor usb keys (Yubikey) using CloudPassage Halo Ghostports.

Method :

a. Login to CloudPassage portal using the password.

b. Open Ghostports using Yubikey

c. Use pem file to ssh into server.

Management of access rights across the network(s) is done by the **CTO**.

Shared access to organization resources by sharing passwords or group passwords are explicitly prohibited.

User access requests, authorization and administration roles should be segregated.

User access requests are subject to formal authorization, periodic review and removal.

Access to the cryptographic keys is restricted to very few custodians.