**PIRAMAL FINANCE LIMITED**

**(Formerly known as Piramal Capital & Housing Finance Limited)**

# Policy on Daksh - Reserve Bank's Advanced Supervisory Monitoring System

May 06, 2025

| | |
|---|---|
| Policy Owner | Compliance Department |
| Policy Location | Mumbai, India |
| Version | V1_ Adoption of Policy |
| Approval Date | May 06, 2025 (Approved by the Board) |
| Next Review Date | May 2026 |
| Supersedes | NA |

### 1.1 Background

The Reserve Bank of India (RBI) has issued guidelines on DAKSH - Reserve Bank's Advanced Supervisory Monitoring System (CO.DOS. RSD. No S438/31-01-105/2023-2024 dated 24th April 2023) for usage by Supervised Entities (SEs) which is applicable to all the Non-Banking Financial Companies (NBFCs) excluding Base Layer NBFCs. This system will provide a web-based interface for RBI and SEs with various functionalities such as inspection planning and execution, compliance submission and monitoring, complaint handling, processing, and the ability to request ad-hoc information via returns.

Piramal Finance Limited ("PFL"/ "Company") is a non-deposit taking Non-Banking Finance Company registered with Reserve Bank of India as NBFC- ICC and engaged in various financial services businesses. In line with the instructions issued by RBI, the Company to ensure a smooth rollout and effective utilization of DAKSH, along with keeping the senior management familiar with its features and workflows of the adopted DAKSH system.

To comply with RBI's directives and to ensure secure and authorized usage of DAKSH, the Company hereby establishes the policy on Daksh.

### 1.2 Objectives

The objectives of this policy are:

1. To put in place a Board approved policy for user creation and maintenance, along with the framework of DAKSH usage.
2. To ensure usage of DAKSH in a secure and authorised manner.
3. To ensure that the Company's' senior management is familiar with features / workflows available in DAKSH.
4. To advise the concerned officials to take necessary action for smooth rollout and effective adoption and utilisation of DAKSH.

### 1.3 Scope and Applicability of the Policy

DAKSH is a web-based end-to-end workflow application through which RBI shall monitor compliance requirements in a more focused manner with the objective of further improving the compliance culture in SEs like Banks, NBFCs, etc. The application will also enable seamless communication, inspection planning and execution, cyber incident reporting, calling of ad-hoc information via returns and analysis, provision of various MIS reports etc., through a Platform which enables anytime-anywhere secure access.

This policy will apply across all aspects of its operations including marketing, loan origination, processing, and servicing and collection activities. The contents of the policy are applicable to

all employees of the company and are aimed at making them familiar with the policy/ processes/ procedures.

The system will generate alerts/notifications to ensure timely actions by RBI and the company.

### 1.4 Guidelines

To ensure the seamless adaptation of Daksh and effectively utilize all its functionalities, the Company will adhere to the following guidelines:

a) Compliance team is entrusted with the responsibility of implementation and usage of the Daksh System. Senior Vice President - Compliance is appointed as the Nodal Officer or point of contact for Daksh related communication with RBI. The name, designation and contact details or any further changes in this respect will be communicated to RBI at daksh@rbi.org.in.

b) The contents shared / provided in DAKSH by RBI and the Company users' need to be protected appropriately against unauthorised distribution or access by all/other users.

c) Ensure that the access to DAKSH is allowed in the Company network and is made from a sanitised environment/desktop/laptop with updated operating system/browsers free from virus /malware. IT / IT security team to provide access points with appropriate anti-virus solution and make access through authorised network. It is recommended to use the company's laptop/device only for submitting any data of the Company via Daksh to RBI.

d) User creation and maintenance along with the framework for mandatory filling of user creation / update / de-activation form and approval for the same from the appropriate authority is to be ensured. The recommended format with mandatory information along with the approving authority is mentioned in the policy at Annexure 1.

e) The information regarding the user creation and maintenance will be readily available, whenever sought by RBI.

f) The specific user access would be granted to a designated employee of the Company who is responsible for that specific role.

g) The Checker access will be granted either to functional heads or a sufficiently senior level employee of the organisation of the responsible department. The respective Checker of each function will be responsible for reviewing the submission made by the respective Maker and obtain relevant approval from functional heads (if the Checker is not the functional heads) as on when required (Refer point no. 2 Maker & Checker Mechanism)

h) The access or credential will mandatorily require to be person specific email ids (non-generic)

i) Roles/access for Daksh will be granted only on need basis to the users.

j) Respective departments will be required to conduct a periodic review of users in DAKSH to ensure the availability of active users with appropriate roles and up-to-date details.

k) Functional Heads or Checker of the respective department will ensure that at any point of time that the roles assigned to users are allowed and matching with user's responsibility in DAKSH.

l) Functional Heads or Checker of the relevant department will be required to update the Company Nodal officer along with Compliance Admin Maker and Checker for any change in the user's status in DAKSH, on account of promotion / transfer / separation from the Company or otherwise, immediately and not later than 2 days from date of the update.

m) Each user will regularly login to DAKSH to check the notifications, alerts and pending items in their queue and take appropriate action.

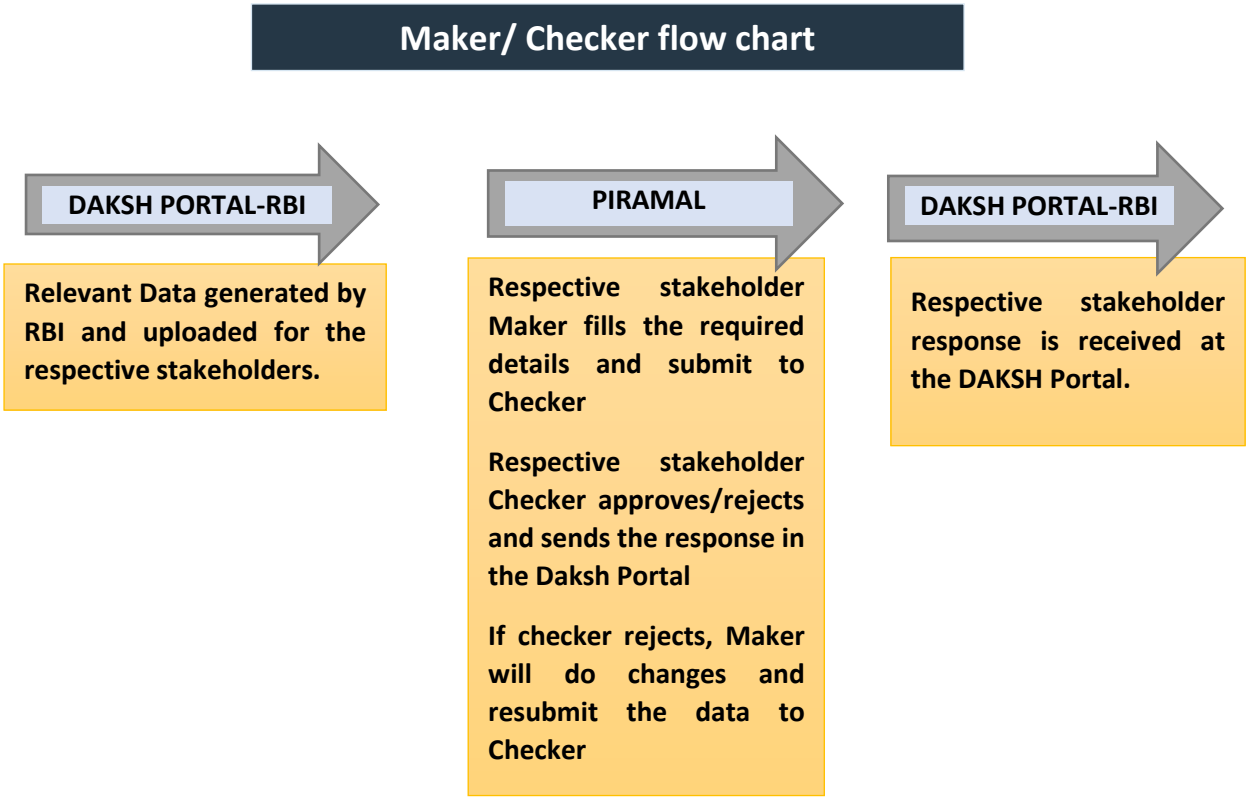
n) IT team & Cyber security team will require to ensure that the DAKSH usage, the process of user creation and maintenance and role assignment is reviewed regularly by the Information System Audit process of the company.

o) Additionally, Compliance team on a quarterly basis, will seek confirmation of compliance/review the abovementioned process being followed from respective Functional Head / Checker.

**2. Maker & Checker Mechanism**

Access to DAKSH and its contents have various security features such as two-factor authentication, captcha, disabling copying and printing of the content, watermarking of pages and implementation of role-based visibility /access of the workflows and information.

Every function in DAKSH is controlled by a Maker-Checker mechanism where the Maker will make an addition/ modification and send it to the respective Checker for approval. The modification made by the Maker will only be reflected post approval by the checker. Rejected values/ responses are sent back to the Maker for relevant modifications.




### 3. DAKSH Compliance Management

a) DAKSH will help the users to maintain and manage the information being used by the different modules of DAKSH and manage the users of DAKSH.

b) The system can be accessed over internet using the link https://daksh.rbi.org.in.

c) The access to the respective modules will be granted to the respective functions mentioned in the Annexure 2 as per the applicability.

d) Each function/department will have to nominate two members from their respective team as users (SE Maker and SE Checker) for accessing DAKSH application.

e) The SE Checker will be required to validate the response for the function on any adhoc questions or submission to RBI/Regulator. Therefore, it is essential that a functional head or a senior level employee of the organisation is granted SE Checker access for the respective function.

f) User update will be approved through duly signed Daksh form and on portal either by the Chief Compliance Officer (CCO) or the Chief Information Security Officer (CISO)

g) For user who are Senior officer or SE Admin Checker, the approval will require to be provided by CXO (CCO / CISO / CRO / CFO / CTO / COO / CEO) level official. Where CXOs are SE Admin Checker the approval must be provided by two members of top

management.

h) The changes in the user's status, /nominations for any reasons on account of promotion /transfer /separation from the Company or otherwise should be intimated to the Company Nodal officer along with Compliance Admin Maker and Checker.

i) RBI has established a helpdesk to assist its users which can be reached at daksh@rbi.org.in and dakshsupportmum@rbi.org.in . Alternatively, users can register their concerns by visiting the website https://helpdeskdaksh.org.in. To assist the users, manuals have been provided in the utility and the company will follow the instructions before approaching the Helpdesk.

## 4. Review of Policy

The Company will review the policy on an annual basis or at earlier intervals, if there any regulatory changes necessitating such interim reviews.

**Annexure 1**

**User Creation/ Update/ Deactivation Form for DAKSH**

| **1. Applicant details** | |
|---|---|
| Name of the Supervised Entity | |
| Name and designation of applicant | |
| E-mail ID of applicant (individual corporate account only) | |
| Registered Mobile Number of the applicant | |
| Whether an employee? | YES (non-employees are not allowed on DAKSH) |
| Employee ID/No. of the applicant | |
| Date of joining the organization | |
| Date of user creation/ update/ deactivation | |
| Reason for user creation/ update/ deactivation | |
| Role(s) to be assigned/ updated to the user.<br><br>SE Admin role to be assigned to sufficiently senior position. | |
| Ticket Reference no. (created in **Ticketing** application) | |
| **End User Acknowledgement** | |
| I shall use the user ID assigned for the intended purpose only and agree to abide by all applicable guidelines.<br><br>Name:<br><br>Signature:<br><br>Date: | |

| 2. To be filled by Approving Officer of SE User (please refer to the guidelines under para 3 below) | |
|---|---|
| Name of the Approver | |
| Designation of the Approver | |
| Applicant's user details and the roles to be assigned to the user verified (Y / N) | |
| Approved (Y / N) | |
| Remarks / Reason for approval | |
| Contact number of the approver | |
| E-mail ID of the approver | |
| Signature and Date | |

**Important guidelines for User on boarding**

1. Generic email accounts are not allowed on DAKSH and only individual corporate email id will be used for the user creation.
2. The user must be an employee of the company.
3. The registered mobile number provided in the DAKSH must belong to the user who is being onboarded.
4. User with role of Admin Checker will be sufficiently senior level in the organisation.
5. The approval for user creation/update/de activation will be approved as mentioned below:
    a) User update will be approved by either the Chief Compliance Officer (CCO) or the Chief Information Security Officer (CISO).
    b) For user who is a Senior Officer or admin Checker, the approval will be provided by the CXO (CCO / CISO / CFO / CRO / CTO / COO / CEO) level official.
    c) For CXOs (CCO / CISO / CFO / CRO / CTO / COO / CEO) and where CXOs are Admin Checker, the approval will be provided by any two members of top management.

**Annexure 2**

**List of departments /functions within the Company:**

| Sr. No. | Departments | SE Maker | SE Checker | Comments (if any) |
|---|---|---|---|---|
| 1 | Compliance | | | |
| 2 | Finance | | | |
| 3 | Credit | | | |
| 4 | Treasury | | | |
| 5 | Risk | | | |
| 6 | Company Secretary | | | |
| 7 | Retail | | | |
| 8 | Corporate & Mid-Market Lending (CMML) | | | |
| 9 | Legal | | | |
| 10 | Information Technology | | | |
| 11 | Information Security | | | |
| 12 | Human Resources | | | |
| 13 | Internal Audit | | | |
| 14 | Credit Administration Department | | | |
| 15 | Wholesale Origination | | | |
| 16 | Asset Management | | | |
| 17 | Value Enhancement Group | | | |