NATIONAL E-GOVERNANCE SERVICES LIMITED

BYE-LAWS

TABLE OF CONTENTS

NATIONAL E-GOVERNANCE SERVICES LIMITED

TECHNICAL STANDARDS

As per Regulation 15 (2) of Insolvency and Bankruptcy Board of India (Information Utilities) Regulations, 2017, the bye-laws of information shall be consistent with, and provide for all matters contained in the Technical Standards, if any.

The IBBI has set forth Technical Standards and issued guidelines for the performance of core services and other services Under the IBBI (Information Utilities) Regulations, 2017, which have provided for the matters in the following bye-laws.

As per the Regulations of the Insolvency and Bankruptcy Board of India (IBBI) to provide a framework for registration and regulation of Information Utilities (IU's) in exercise of the powers conferred by sections 196, 209, 210, 211, 212, 213, 214, 215, 216 read with section 240 of the Insolvency and Bankruptcy Code (IBC), 2016 (31 of 2016), (As amended upto 25th July 2019), National E-Governance Services Limited (NeSL), makes the following Bye-laws.

CHAPTER - I

1. TITLE AND COMMENCEMENT

Pursuant to the requirement of Regulation 15 of Insolvency and Bankruptcy Board of India (Information Utilities) Regulations, 2017 (Hereinafter referred to as "Regulation(s)"), National E-Governance Services Limited hereby makes the following Bye-Laws.

a) These bye-laws shall be called the Bye-Laws of National E-Governance Services Limited.

b) These bye-laws shall come into force with effect from 25th September, 2017.

c) Subject to the provisions of Insolvency and Bankruptcy Board of India (Information Utilities) Regulations, 2017 as may be amended from time to time and receipt of approval from the Board, NeSL may amend, add to, alter, modify or repeal any of the provisions of these Bye Laws.

CHAPTER - II

2. DEFINITIONS

Unless the context otherwise requires, in these bye-laws

a) "adjudicating authority" shall have the meaning as defined in section 5(1) and section 79 (1) of the code.

b) "ancillary services" means services other than the core services, which NeSL may render in accordance with these bye-laws, subject to the provisions of the Code and IU Regulations;

c) "code" means the Insolvency and Bankruptcy Code, 2016;

d) "company secretary" shall have the meaning as ascribed to it under section 2(24) of Companies Act, 2013;

e) "core services" shall have the meaning as ascribed to it under section 3(9) of the Code;

f) "digital Signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of Section 3 of the Information Technology Act, 2000;

g) "digital signature certificate" means a digital signature certificate issued under sub section (4) of section 35 of the Information Technology Act, 2000;

h) "Exit Management Plan" means a plan approved by the Governing Board for transitioning its users' information to another information utility as per the requirement of Regulation 39;

i) "e-sign means authentication of any document by signing it electronically through the "Aadhaar" based e-sign process;

j) "IBBI" means the Insolvency and Bankruptcy Board established under the Code;

k) "Independent director" shall have the meaning as ascribed to it under section 2(47) of Companies Act, 2013;

l) "Financial information" shall have the meaning as ascribed to it under section 3(13) of the code;

m) "IU Regulations" means the Insolvency and Bankruptcy Board of India (Information Utilities) Regulations, 2017 including any amendments made thereon from time to time;

n) "Insolvency professional" shall have the same meaning as defined under section 3 (19) of the code including interim resolution professional as the case may be;

o) "NCLT" means the National Company Law tribunals set up by the Ministry of Corporate Affairs;

p) "NCLAT" means the Appellate Authority for all the NCLTs;

q) "NeSL platform" means the electronic platform through which NeSL shall provide its services;

r) "person resident in India" has the meaning assigned to it under the Foreign Exchange Management Act, 1999;

s) "porting" means the process by which an information utility gets information from any other central registry or any other information provider approved by the Board;

t) "services" means core services, ancillary services and support services;

u) "support services" means services that users may require to effectively avail the core services or ancillary services, such as technical support and user queries;

v) "user" means any person who is registered with NeSL as per Regulation18 to avail any of the services of NeSL;

w) "unique debt identifier/ UDI" means a unique number assigned by NeSL to every debt, information of which has been submitted to NeSL.

x) "unique identification number/UIN" means a unique number assigned by NeSL to every user on registration with NeSL.

y) All words and expressions used but not defined in these bye-laws but defined under the Code or the IU Regulations, shall have the same meaning respectively assigned to them under the Code and the IU Regulations and the Companies Act, 2013 as the case may be.

CHAPTER – III

3. CORE SERVICES – Standard Terms of Service

In accordance with Regulation 13(2)(b), the standards for authentication and verification of information of NeSL are governed by the following aspects:

a) NeSL shall strive to offer the various "Core Services" as defined under this bye-laws to the best of its abilities and in a fair, transparent and efficient manner without discriminating between different users, in accordance with the Code.

b) NeSL shall not deny services to any person on the basis of place of residence or business or type of personality.

c) NeSL shall strive to provide qualitative and error free services to its Users.

d) NeSL shall deliver the services through its electronic platform area, as far as possible, during all times of the day.

e) NeSL shall be upfront with the user and ensure that the user is informed of the terms and conditions covering the services and fee structure for its various services and also ensure that the same is displayed on its website.

f) NeSL shall charge uniform fee for providing the same service to different users.

g) Any increase in the fee structure of NeSL shall be notified to the user at least 3 months before the effective implementation date.

h) NeSL shall put in place suitable Grievances Redressal Mechanism operated on an electronic platform and ensure prompt redressal of grievances.

i) NeSL shall provide services to a user based on its explicit consent.

j) NeSL may provide services incidental to the services along with "Core Services" with the permission of the Board.

k) NeSL shall always comply with the applicable Technical Standards, while providing these services.

CHAPTER – IV

4. REGISTRATION, IDENTIFICATION AND VERIFICATION OF USERS

a) All users of NeSL's services shall register themselves with NeSL.

b) All users shall fill in the required registration form put on the website of NeSL.

c) All users shall submit the basic Identification documents and other documents as may be requested by NeSL.

d) NeSL shall verify the identity (ID) of the user registering with NeSL with prescribed Identity documents in accordance with the Technical standards or Regulations.

e) All users registering with NeSL shall pay the required fee prescribed by NeSL in advance or as may be agreed through an Agreement with NeSL that is executed in advance;

f) NeSL rules out registering of a user already registered with any other IU or already registered with NeSL in the normal course of business;

g) NeSL shall therefore, before opening a user account or registering a prospective user with NeSL, run a de-duplication process on its own systems and on the systems of other information utilities to ascertain that the applicant has not previously registered with any other information utility;

h) Where NeSL is unable to access the systems of other information utilities to run such a process immediately, NeSL shall keep the account creation on hold. As soon as NeSL is able to access the systems of the other information utility, it shall rerun the de-duplication process.

i) NeSL is authorised to use the data furnished by such person to run a deduplication process on its own systems and with the other information utilities.

j) On successful registration NeSL shall assign a Unique Identification Number (UIN) to every user;

k) NeSL shall maintain a list of the:
   - registered users
   - the unique identifiers of the registered users; and
   - the unique identifiers assigned to the debts under Regulation 20.

l) NeSL shall display the names of the registered users and their UIN for the use of other IUs as per Regulation 18(6)(b);

m) NeSL shall provide a registered user a functionality to enable its authorised representatives to carry on the activities of submitting information and accessing such stored information on its behalf.

n) The digital signatures, as defined under the Information Technology Act and as permitted in UIDAI Rules such as through digital signature certificates or Aadhaar based e-sign, are at the core of the NeSL processes and public keys will be stored as part of registered user data for future reference or validation.

o) NeSL shall monitor the registration and user administration activities.

p) NeSL shall undertake the following processes for Registration, Identification and Verification of Users:

i. Capture the minimum required information as in accordance with the Technical Standards covering identity and contact details

ii. Conduct a de-duplication check across all IUs to ensure that the User is not already registered

iii. Verify the identity of the User against the original issuer of ID

iv. Upload the Digital Signature Certificate (if available) and its verification with the certifying authorities

v. Receive an acceptance from the User, of the terms of usage as formulated by the concerned Information Utility

vi. Receive the fees as published by the IU on its website

vii. Allot the Unique Identifier Number (UIN – described under the Technical Standards pertaining to Unique identifier for each record and each user)

viii. Issue the user ID and password to the User

ix. NeSL shall provide an alternative mechanism "(eg. the use of Digital Signatures by the authorised Indian Representative or power of attorney holder)" to accept other supporting documentation for non-resident Indians or foreign individuals.

x. For a legal entity seeking registration, NeSL shall collect the registration information of the entity as well as its authorised representative who shall be undertaking the registration process. In furtherance thereof, the following details shall be captured:

- Name of entity
- Type of person/ Legal constitution (e.g. Company, LLP, Partnership, HUF, Society)
- Indian/ Overseas status
- PAN as the primary ID
- CIN/ LLPIN (if registered with MCA)
- Date of incorporation
- Representative person's full name
- Representative's designation
- Primary & Alternative Email ID
- Primary Mobile number
- Alternative Mobile number
- Landline number (if available)
- Registered office address with PIN Code
- Communication/ billing address with PIN Code

xi. NeSL shall perform a de-duplication check first within its own database and also against the shared list of registered users of other IUs (as provided under Regulations 18(6)(b) to check if the legal entity is already registered). This shall be on the basis of the PAN of the legal entity. If a match is found, the user shall be informed and asked to login. If the de-duplication returns 'not match', NeSL shall verify the PAN with the issuing authority (IT Department database).

xii. For the legal entity's authorised representative, the Identity documents shall be crosschecked with the issuer department. Alternatively, his/her identity will be verified using digital signature certificate.

xiii. Upon completion of the registration process, the authorised representative of the legal entity shall submit a Digital Signature Certificate (DSC) of the legal entity, at the earliest opportunity or should opt for Aadhaar based e-sign.

xiv. Where Aadhaar e-sign is not opted for, DSC shall mandatorily be submitted before the digital signing of a submission or an authentication can be performed:

- In case of a legal entity, NeSL shall verify such DSC, when submitted, to check its validity.
- Where the DSC information does not match with the registration data, or the DSC is issued in personal capacity or the DSC is not submitted, the person seeking registration shall be required to upload a soft copy of the supporting documents from the organisation to NeSL

in order to confirm that the person being registered is authorised to represent the legal entity.

- In case of authorisation based on a Power of Attorney, the authorization shall be checked against the Resolution of the Board. In such a situation, NeSL shall be required to check the contents of the Board Resolution and then approve the registration request.

- Email ID and mobile number provided during the registration of a legal entity shall be verified by sending an appropriate message with OTP/ verification link to the email ID and the mobile number. NeSL shall use only verified contact information. No verification of postal address is required to be performed by NeSL.

xv. Before the completion of registration, the person being registered must accept the terms of usage as specified by NeSL. This shall also apply to individuals accessing the database upon completion of Identity validation.

xvi. NeSL shall send a confirmation email on the completion of the registration process. NeSL shall also be required to issue a Login ID and a Password through the preferred contact mode of email ID or mobile number for the legal entity user. When the authorised person logs into NeSL portal for the first time, he/she shall need to provide a second factor as credential namely, date of incorporation and shall be required to change the password on first use.

xvii. The authorised representative of the legal entity can access all NeSL services on behalf of the legal entity by using the Login ID and password. For legal entities, the first registered representative user will be allowed to create additional users by using the User Administration function in the NeSL portal. Creation and administration of other users shall be the responsibility of and shall be under the direct control of the legal entity's registered representative. NeSL is not required to verify the identity of any additional users created under the authority of the registered authorised representative of the entity.

xviii. Where a legal entity (such as banks or other creditors) seeks to implement a server based automated process for digital signature and submission, a specific type of DSC meant for installation on server shall also be registered under a person belonging to the legal entity.

xix. NeSL shall monitor the registration and user administration activities including those being performed by the legal entities, in order to identify any unusual pattern such as accounts remaining dormant for a long period.

CHAPTER – V

5. UNIQUE IDENTIFIER FOR EACH RECORD AND EACH USER

a) NeSL shall maintain a list of the registered users, the unique identifiers of the registered users, and the unique identifiers assigned to the debts under Regulation 20.

b) NeSL make the list under clause 5 sub-clause (a) available to all information utilities and the Board.

c) PAN number shall be directly used as UIN for all legal entities and also for individuals depending on the type of person, where PAN is not applicable or possible to be used, an alternative Identity details field shall be used as the identifier or a UIN issued by IU

d) A key benefit of using the ID itself as the UIN is that there is no need for the creditors (and for the users) to store any new number issued by NeSL in their respective systems. All systems at the creditors' end already have provisions for PAN and Identity fields. Hence, implementation of the NeSL interface will be easier. Further, even users do not need to remember any new number assigned to them.

e) For non-resident Indian individuals or foreign nationals/entities, not covered by Identifier, as above, NeSL shall assign a new number since no fixed document type is applicable.

f) Unique Debt Identifier (UDI) - UDI is planned as a combination of the creditor's identity (UIN) combined with the loan account number allotted by the creditor. Prefixing of creditor identification (PAN) is necessary for uniqueness of UDI since it is possible that two creditors may have issued the same loan number.

g) In most situation, the creditor will be a legal entity with PAN (10 digit) as the UIN. However, in some situation (e.g. P2P or Operational Credit) an individual can also be a creditor. In such situation too PAN may be used as the preferred UIN to ensure uniqueness. Only in some exceptional situation an alternative Identity details can be used as UIN.

CHAPTER – VI

6. SUBMISSION OF INFORMATION

a) A registered user shall submit "financial information" as defined under Section 3 (13) of the IBC.

b) The user may submit information using different methods devised for this purpose by NeSL.

c) The User shall submit the information in Form C under Regulation 20 as advised by NeSL including any changes as may be advised from time to time. A single submission file may have data about multiple debts including defaults, i.e. submitter identity, other party information and security information is to be part of the same file containing the debt information which also includes outstanding liabilities.

d) The 'other party' section of Form C will be repeated multiple times in the same file depending on number of parties connected to the debt.

e) Similarly, security details will also be repeated as many times as there are securities linked to the same debt. Where a single security is linked to multiple debts, each record of debt should accompany the same security data as linked information.

f) The section on default (Form C in Annexure) will be undertaken only at the time of reporting of default.

g) The submission of information to NeSL shall be done with the digital signature of the submitter. The Digital signature should be of requisite class as specified in the standards for security of information or can be the Aadhaar based e-sign.

h) Documents for a debt or security can be submitted at any time. Default can be reported at any time by the creditor in Form C. Such documents shall be supported across multiple formats including PDF and scanned image files. Each supporting document for security shall have security identifier reference.

i) NeSL can allow multiple modes of submission covering batch upload of multiple records (e.g. manual upload of file or automated server to server file transfer using Simple Object Access Protocol based API service or push from creditor's server to a designated Secure Shell File Transfer Protocol server) or even screen based entry of one record at a time.

j) Any error, if comes to the notice, can be marked erroneous by the submitting party only.

k) On receipt of the information, NeSL will assign a Unique identifier to the information including records of debt. An acknowledgement shall be issued to the submitting party on receipt of any submission of data/ document by NeSL.

l) On receipt of information, NeSL shall also acknowledge its receipt and notify the user the UIN, the terms and conditions of authentication and verification of information and also a consent framework for permitting third parties to access the information.

m) Insolvency Professional (IPs) registration particulars with IBBI and the appointment of the IP as the resolution professional by the adjudicating authority will be verified by NeSL before permitting submission or access of information by them.

n) Default Reporting: Creditor(s) may report default of a debt with reference to a specific debt in the following manner:

   i. For reporting of default, Data as per section on Default in Form C shall be submitted. Creditor may upload/ submit any supporting documents as proof of default along with the data of default. The debtor or its authorised Auditor can submit unpaid invoice or account or cash-flow statements as electronic documents (PDF, scanned documents etc.), if any. This shall be submitted with reference to debtor unique identifier (i.e. PAN). The email of the debtor shall be furnished as mandatory. Such submissions can be made directly to NeSL.

   ii. Alternatively, NeSL may consider porting such statements already submitted by the debtor or its Auditor to Ministry of Corporate Affairs in digitally signed mode, thereby avoiding the need for direct submission to NeSL.

o) Submission of other information by IRP:

   i. The IRP must be a registered person like any other submitter of information

   ii. NeSL shall check that the IRP has a valid registration number issued by IBBI. This should be validated using an API provided by IBBI.

   iii. Based on court order documentation made available to NeSL, NeSL shall link a debtor to an IRP. The consent framework could be another route for the IRP to get access to the records of the debt in NeSL.

   iv. All submissions of IRP will be with reference to debtor unique identifier. Submissions by IRP will be in the form of various documents related to the debtor. Basic metadata about each submitted document will be submitted along with such documents.

v. NeSL can allow multiple modes of submission covering batch upload of multiple records (e.g. manual upload of file or automated server to server file transfer using Simple Object Access Protocol based API service or push from creditor's server to a designated Secure Shell File Transfer Protocol server) or even screen based entry of one record at a time.

vi. Periodic updates to the financial information can be provided in same Form C format as used for the original information submission since this approach may be easier for various submitting parties. Banks/creditors may find it difficult to submit only incremental changes since the last submission and also such information may only give a partial information to authenticating parties.

p) Exception handling: The submitted information will be rejected by NeSL if:
   i. One or more records of a bulk submission file are found not conforming to the specified format or are missing the mandatory fields.
   ii. Digital signature is found missing, invalid or expired.

q) Error-Marking: If any information is noticed to be erroneous, whether before or after it is authenticated, the submitting party shall mark the record as erroneous giving reasons and also arrange for corrected data submission as a new update record. Only the submitting party and no other party will be permitted to mark information erroneous. Any user registered under the submitting party, which is a legal entity, will be allowed to mark information submitted by the same legal entity as erroneous.

r) Issuing of acknowledgement: The acknowledgement shall be issued on receipt of the valid submission without waiting for authentication to be performed. This will be sent to the registered and verified email ID of the submitting party. The acknowledgement should specify key information submitted, including receipt date, unique identifier allotted by NeSL as applicable, terms & conditions of authentication and verification. The terms and conditions for authentication and verification should contain NeSL's plans and means of approaching the concerned parties for obtaining authentication.

s) NeSL shall ensure that the submitting user is able to download, if needed, the acknowledgement as a PDF digitally signed by NeSL, at any point of time.

t) NeSL shall allow only financial information as provided under the Code related to a debt, parties to the debt, security, default etc. to be submitted and stored.

u) A user may access information stored with NeSL through any information utility.

CHAPTER – VII

7. AUTHENTICATION & VERIFICATION OF INFORMATION - OVERALL PROCESS

a) Verification in this context implies the process of accessing and viewing the information presented for authentication before the actual authentication of information is performed by affixing a digital signature.

b) NeSL shall forward the information received from the submitters for authentication.

c) Electronic link to NeSL's website/ mobile, etc. will be sent through the registered email Id/mobile etc., clicking on which all information to be authenticated by the other parties will be displayed for verification and authentication.

d) The user can authenticate the entire information or may disagree with all or part of the information. NeSL shall permit a time period for authentication as directed by the Technical Standards. Status of authentication or otherwise will be sent to the submitter of information.

e) The persons authorized to authenticate the information shall affix their digital signature certificate or the Aadhaar based e-sign when the information provided by the submitter is placed on the platform of NeSL. NeSL shall verify the identity of the authenticator.

f) NeSL only facilitates the authentication process and does not carry any responsibility if the other parties do not authenticate or dispute the information of the submitter and/or the other parties.

g) All parties may settle such issues by contacting the respective counterparties directly.

h) Retrieval and Dissemination:

i. Access to information shall be permitted strictly according to Regulation 23 (1, 2 & 3).
ii. NeSL shall take all necessary caution to verify the identity of the requester and his eligibility to access the information he wants to access.
iii. Authorised persons of the users will be permitted to access information related to the authoriser.
iv. A consent framework is put in place separately for allowing third parties to access information. Details of the same will be put in NeSL's website covering usage terms.

CHAPTER – VIII

8. AUTHENTICATION & VERIFICATION OF INFORMATION - DETAILED FLOW

As per Regulation 13(2)(g) and 13(2)(h) of the IU Regulations, 2017, the standards for authentication and verification of information are governed by the following aspects in IU's and in accordance with these:

a) Facilitating authentication of information from all concerned parties shall be the core function of an NeSL.

b) NeSL shall present information to the concerned parties, for verification and authentication by affixing digital signature, based on the information received from submitter without any changes introduced by IU.

c) NeSL shall maintain status of authentication for each record of information including any dispute.

d) NeSL shall preserve each artefact used during submission and authentication in its original form at the time of affixing digital signature, for the purpose of checking veracity at any time.

e) On authentication of default, NeSL shall inform all related parties to the debt and also all creditors related to the debtor.

f) When a link for authentication is presented by NeSL, the party concerned shall register first if not done already and then proceed with verification and authentication of the information. Individual persons need to be verified against their Identity credentials.

g) Any registered user, on logging into/ accessing the NeSL portal, shall be presented with all pending authentication requests in the relevant section of the portal.

h) The authentication page containing the information will be displayed by NeSL to the authenticating person only after verifying identity and credentials of the person from the registration information, whether registered with NeSL or a different IU.

i) NeSL shall ensure the information presented for authentication is as received in submitted file or extracted from the submitted information, without altering any information elements. The authentication page must contain an undertaking by the authenticating person confirming that he/she has verified the information presented before affixing digital signature/e-sign. No digital signing is allowed without presenting the information contained in the underlying data file or document to the authenticating person.

j) When the authenticating party confirms the information and digitally signs the same, NeSL shall ensure that the digital signature is based on and affixed to an artefact (data file/ document) as was presented to the authenticating party for verification:
   i. For users representing a legal entity, such user is expected to use digital signature certificate (DSC) that has been registered with NeSL and linked to the legal entity or the Aadhaar e-sign of the authorised user of the entity or any additional user created under his/her authority and control.
   ii. For individuals (e.g. debtor in a retail loan or an individual guarantor), Aadhaar based e-Sign may be used in his/ her individual capacity.

k) NeSL shall preserve each piece of data file or document, used for digital signature during submission and authentication, without any alteration so that such artefacts are always verifiable against the digital signature at any point of time in the future to support non-repudiation.

l) When the authenticating party disagrees with or disputes a part of or entire information presented, NeSL shall provide for obtaining reasons for dispute.

m) Authenticating person's signature will be affixed on the information file which will include dispute flag and reasons for the dispute along with the information presented. NeSL shall notify the submitting party as soon as a dispute is recorded by any concerned party and also make such information available as an exception report.

n) If the authentication request, sent to the concerned party, remains unauthenticated beyond 15 (fifteen) days or till an updated information under the same UDI is received, whichever later, the authentication will be considered to be a *'failed authentication'* treated as 'expired' and the same record will not be available for authentication by the same party subsequently. For any default information, however, process as specified under IU Regulation 21 will apply.

o) The different 'status' of authentication which maintained by NeSL for each record and each party shall cover:
   i. ***'Not presented':*** Normally IU will immediately present any received information to the concerned parties for authentication. Hence this status will be transient in nature till a mail/ message is sent out to the concerned parties.
   ii. ***'Pending'***: when the concerned party is yet to undertake authentication.
   iii. ***'Failed Authentication':*** if the specified time limit of 15 days is exceeded or an updated submission of the same UDI is received, whichever later and treated as *'expired'.*

iv. ***'Authenticated'***: when the concerned party verifies and accepts the information presented and then affixes digital signature or e-Sign to the artefact as presented, without any change.

v. ***'Disputed'***: when the concerned party disagrees/disputes a part of or the entire information presented and then affixes signature or e-Sign to the artefact as presented, without any change.

vi. ***'Deemed to be Authenticated':*** Applicable only in case an information of default is not responded by a debtor even after three reminders as per Regulation 21.

A colour coding scheme for different 'status' of authentication of information of default as provided under Regulation 21 needs to be maintained by an IU for each default loan record.

p) Authentication status will be maintained in relation to each record of information and each concerned party.

q) If submitted information of default is authenticated (i.e. Authenticated, Disputed or is Deemed to be Authenticated) by the concerned party or by any third party through any standard mechanism as notified by the Regulator from time to time, NeSL shall send a default confirmation alert to the following along with information of the debt and the debtor:

i. All parties linked to the defaulted debt (i.e. creditor, guarantors, co-applicants) at the respective registered contact email and mobile numbers.

ii. All creditors linked with the same debtor in any other records of debt maintained within NeSL.

iii. All other IUs, to allow each such IU to inform creditors related to debts held by such IU pertaining to the same debtor.

r) Information of default

i. NeSL shall expeditiously undertake the process of authentication and verification of information of default as soon as it is received.

ii. NeSL shall deliver the information of default to the debtor seeking confirmation of the same within the time specified in the Technical Standards.

iii. NeSL shall remind the debtor at least 3 (three) times for confirmation of information of default, in case the debtor does not respond, allow three days each time for the debtor to respond.

iv. NeSL shall deliver the information of default or the reminder, as the case may be, to the debtor either by hand, post or electronic means at the postal or e-mail address of the debtor

- registered with the information utility by him, failing which,
- recorded with any other statutory repository as approved by the Board, failing which,
- submitted in Form C of the Schedule

v. On completion of the process under sub-regulation (2), the information utility shall record the status of authentication of information of default as indicated in the Table below:

Table Sl. No.	***Response of the Debtor***	***Status of Authentication***	***Colour of the Status***
1	Debtor confirms the information of default	Authenticated	Green
2	Debtor disputes the information of default	Disputed	Red
3	Debtor does not respond even after three reminders	Deemed to be Authenticated	Yellow

CHAPTER – IX

9. DATA INTEGRITY

As per Regulation 13(2)(i), 13(2)(k) and 13(2)(l), aspects pertaining to data integrity have to be followed in accordance with the prescribed technical standards.

Security of the system:

a) NeSL shall put in place an Information Technology (IT) security policy and Cybersecurity policy, detailing all preventive measures to mitigate data security risks.

b) The data center and disaster recovery design and operations should conform to performance standards and operational standards, such as Uptime Institute's Tier Standards with a data center rating of Tier 3 or above. NeSL service shall be hosted in a data center and DR facilities shall be within India and be governed by its applicable laws.

c) For security standards, NeSL shall consider relevant security frameworks (including cybersecurity) used by regulatory bodies like Reserve Bank of India (RBI) and Securities & Exchange Board of India (SEBI). NeSL shall consider Information Security standards such as ISO 27001 for adoption.

d) The data should be transferred using secure, authenticated and industry-accepted encryption mechanisms to avoid malicious users intercepting the data and gaining unauthorized access

e) NeSL shall establish adequate security systems to protect the data processing systems against unauthorised access, alteration, destruction, disclosure of information.

f) Encryption of stored data may be restricted to more sensitive columns, suitable access control measures to be put in place to prevent unauthorised access to any internal or external persons.

g) Business continuity of IT systems should be ensured through Disaster recovery (DR) and NeSL shall put in place a Business Continuity Plan (BCP) and get it approved by IBBI. An RPO (Recovery Point Objective) of 15 minutes and a RTO (Recovery Time Objective) of 1 business day shall be adequate considering the nature of NeSL activity. The same should be reviewed periodically by NeSL.

h) The Data Centre and DR design shall include multi-tier security features like access control to only authorised personnel with proper approval mechanism, audit log for support/ service engineers and video monitoring.

i) Since application is exposed to internet, application security testing shall be ensured. Application shall also be tested for security vulnerability. Secure coding standards shall be enforced to ensure that such vulnerabilities are not created in the first place and audit of the code shall be undertaken to ensure the same.

j) Secure data access shall be enabled through ***sftp*** for bulk transfer and ***https*** for browser based access.

k) Network security shall be enforced using Firewall, Intrusion Detection/ Protection System, Anti-bot, Antivirus/ Anti malware/ Anti-Spam

l) NeSL shall establish a robust capacity planning policy.

m) Regular security and software audits by 'Cert-in certified auditors' shall be conducted. NeSL shall submit reports of system and IS audit to IBBI.

n) NeSL shall establish efficient information security through SIEM capabilities. The lessons learnt should serve as a policy review tool to prevent recurrence and build safeguards on information assets and infrastructure.

o) NeSL shall build resilience in every sphere of IT function viz., system development, testing, deployment, production, monitoring, etc., with formal review process to mitigate hidden risks.

p) NeSL shall ensure that there is a role and reporting segregation between Chief Technology Officer and Chief Information Security Officer to avoid conflict of interest.

q) To ensure better availability, submission of data simultaneously to both sites can be considered so that data is not lost even if a site goes down before replication can happen.

r) A set of policies and procedures shall be adopted to enable the recovery or continuation of service following a natural, human-induced disaster or any technological issues.

Security of information/ Information Integrity:

a) Change Management policies for software releases shall be enforced.

b) Verification of the identity of the person registering shall be done through generally accepted, easily verifiable and reliable Identity documents issued by government agencies before allowing the registration. Before registering a user, NeSL shall ensure that the same user is not registered in any other IU.

c) Email address and mobile number shall be verified.

d) Validation of the record of debt in the system of IUs to ensure that every debt record is unique before it is stored in NeSL.

e) NeSL shall accept only digitally signed data/ information from the submitter. The digital signature shall be Class 2 or above.

f) All information artefacts (data/ documents) submitted to NeSL shall be stored in the original form for any future reference or verification.

g) NeSL system shall maintain an Audit Trail of users, such as IP address, date and time of access

Storage of information:

a) NeSL shall store all information in a facility located in India. The facility shall be governed by the laws of India.

b) The financial information collected by NeSL shall be stored securely, duly ensuring adequate safeguards and security as prescribed in the Information Technology Act, 2000.

c) Access to data shall be provided only to authorised persons after verifying their identity through log-in credentials.

d) Suitable Business Continuity Plan & Disaster Recovery Mechanisms shall be put in place by NeSL. Appropriate Security Audits shall be ensured by the Information Utility periodically.

CHAPTER – X

10. CONSENT FRAMEWORK FOR PROVIDING ACCESS TO INFORMATION TO THIRD PARTIES

a) As per Regulation 13(2)(j), the consent framework for providing access to information to third parties are in accordance with the Technical standards and are as follows:

For ***individuals***, the consent artefact, once it is fully mature and developed, shall capture the following details:

i. Primary Identifier of the individual to whom the consent is provided
ii. Name (as Per Aadhaar)
iii. Start date of authorisation
iv. End date of authorisation
v. Reason for authorisation
vi. Consent for Debt Id: Values could be 'ALL' or 'specific' debt numbers (comma separated if multiple debts)

b) For ***legal entities***, the consent artefact, once it is fully mature and developed, shall capture the following details:

i. Primary Identifier of the representative to whom the consent is provided
ii. Name (as per the Primary Identifier)
iii. Start date of authorisation
iv. End date of authorisation
v. Reason for authorisation
vi. Consent for Debt Id: Values could be 'ALL' or 'specific' debt numbers (comma separated if multiple debts)

c) **Access to information:**

NeSL shall allow the following persons to access information stored with it –

i. the user which has submitted the information;
ii. all the parties to the debt and the host bank, if any, if the information is of the categories in section 3(13) (a), (c) and (d) of the IBC;
iii. the corporate person and its auditor, if the information is of the categories in section 3(13) (b) and (e) of the IBC;
iv. the insolvency professional, to the extent provided in the Code;
v. the Adjudicating Authority;
vi. the Board;

vii. any person authorised to access the information under any other law; and

viii. any other person who the persons referred to in (a), (b) or (c) have consented to share the information with.

d) NeSL shall in all cases enable the user to view the date the information was last updated, the status of authentication, and the status of verification.

e) NeSL shall provide information to the Adjudicating Authority and Board free of charge while providing access to the information.

f) **Accessing information stored with other information utilities:**

NeSL shall provide a functionality to enable users to access information stored with any information utility, which they are entitled to access. The functionality shall enable other information utilities to provide access to information to the user directly. The functionality shall ensure privacy and confidentiality of information.

CHAPTER - XI

11. RISK MANAGEMENT FRAMEWORK

Risk management is "a process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organisation's objectives" (Institute of Internal Auditors, Florida).

As per Regulation 13(2)(m), NeSL shall establish an appropriate risk management framework, as proved by the Board, detailing the risks likely to be faced by it in its day to day operations and business and the methods to mitigate the same, in accordance with the Technical Standards, which shall provide for the following matters:

Key Considerations:

NeSL's risk management framework shall:

- Define processes to identify, assess, and manage all the risks that may affect the activities of NeSL;
- Encourage high level of accountability across the organisation;
- Establish open and transparent communication across the entire organisation; and
- Identify persons responsible for managing the risk and controls in place.

a) **Identification of Risk:**

i. The objectives of the organisation shall be clearly stated.

ii. The risk management framework shall identify the various risks, the sources of the risks and controls to be put in place for containing such risks.

iii. All potential risks affecting the various operations/services shall be identified.

iv. External factors affecting the objectives of the organisation like technological changes/ obsolescence, regulatory changes, risks embedded in outsourced services/vendors etc. shall be considered.

v. Internal risk factors at the organisational level including interruptions in IT systems, man-made or natural disasters affecting the operations shall be considered.

vi. Employees shall be encouraged to report incidents, however small they are, to enable to build up data of incidents which will be useful in identifying the risks.

b) **Assessment of Risk:**

NeSL shall –

i. Identify and establish efficient and effective physical and electronic assessment controls to avoid unauthorised access to the systems at NeSL.

ii. Assess the identified risks as to what will be the impact if that risk has to occur through probability and impact study.

iii. Assess the risks based on the likelihood and impact on the objectives of the organisation.

iv. Assess the impact of the risk on earnings, reputation, business and legal implications.

v. Rate the assessed risks as Low, Medium or High depending on the probability and impact.

c) **Management of risk:**

i. Risks that cannot be shared, transferred or avoided shall be managed

ii. NeSL shall draw up a Business continuity plan and disaster recovery plan considering the importance of the services it is offering to all users.

iii. As part of the Business Continuity Plan, NeSL shall conduct an analysis of the impact on its business, of potential disruptions, tolerance levels for such disruptions and the resources required to continue the business within such tolerance levels.

iv. Decision to share the risk through insurance cover shall be decided by the Board.

v. A risk register to document various risks under People's risk, Operational or Process risk, IT risk, Compliance risk etc., shall be prepared.

vi. For managing People's Risk, NeSL shall initiate steps to enforce a culture of integrity & honesty, monitoring work, providing training/ retraining for enhancing skills, etc.

vii. For managing Process Risk, NeSL shall initiate steps to engage professionals to make an independent assessment of risk within the systems & procedures in order to standardise

and de-risk procedures and improve systems through improvements and institute appropriate controls.

viii. For managing Technology Risk, NeSL shall put in place, reliable, recoverable and secure systems, Robust Access Control Systems for Data Security, Network intrusion prevention Systems, Business Continuity Plans by establishing Disaster Recovery Centre/Near Data Centre.

ix. NeSL shall get the VAPT (Vulnerability and Penetration Testing) Tests done at periodical intervals, Systems Audit done by CISA qualified external auditors on its IT Framework/interface, and Information Security Audit.

x. NeSL shall adopt Quality Standards and get Quality Standards Certifications/ ISO Standards Certifications etc.

xi. NeSL shall ensure that risk is managed by persons close to the risk e.g. unit head, business head, CTO/ CISO etc.

xii. NeSL shall test controls on a periodic basis to ensure effectiveness of the controls.

xiii. Findings of Audits shall be placed before the Board of Directors of NeSL which has the overall supervisory responsibility and the Board shall ensure that proper risk management practices are implemented.

d) **Responsibility in risk management**

i. The CEO shall have the overall responsibility and ensure that every employee of the organisation is aware of risks affecting the operations.

ii. Senior management of the organisation shall put in place risk management policy and processes containing the organisation's view on risks and identifying various risks like operational risk, IT risk, Compliance risk and controls for the same. They shall review the risk management process at regular intervals.

iii. NeSL shall also appoint an external auditor having the requisite qualifications for conducting an audit of the information technology framework, interface and data processing systems established as part of the risk management plan. The external auditor

shall conduct annual audits of such frameworks and systems. The external auditor shall submit, directly, the audit report prepared by it to the Audit committee.

e) **Monitoring the risk management process**

i. A Disaster Recovery Plan clearly outlining the processes and procedures for recovering and protecting information in the event of any unforeseen man-made or natural disasters shall be made. This Plan shall include processes to recover access to the software, data and/ or hardware that are needed to resume the performance of the normal and critical business functions post the occurrence of such disasters within reasonable time.

ii. NeSL may also consider using the services of professional hackers to check the robustness of the security systems and firewall.

iii. IT security systems and processes shall be audited by a CERT-IN certified external auditor.

iv. The Governing Board shall supervise the compliance risk and the external Auditor shall give its report to the Governing Board .

v. The CEO shall report to the governing board on a quarterly basis the functioning of risk management framework and exceptions found, if any.

vi. Audit committee, in the absence of a risk committee, shall review the IT audit report to ensure that the controls are functioning effectively.

vii. NeSL shall ensure provision of core services during disasters and emergencies and also ensure that business continuity plans include disaster recovery sites.

CHAPTER - XII

12. PRESERVATION & PURGING OF INFORMATION

Information shall be preserved and purged as per Regulation 13(2)(q) and 13(2)(r) and in accordance with the Technical Standards.

a) All information maintained by NeSL will be in electronic form only.

b) NeSL shall choose its internal data store design and data format. However, such storage format should not inhibit exchange or transfer of data between IUs or inter-operability of IUs in any manner.

c) Any artefact, in the form of data file or scanned /other documents, which are digitally signed by a user of NeSL, must be preserved in the original form which was used for digital signature. This is to ensure that the digital signature is verifiable with the document anytime in the future.

d) Digital signature should be stored with the information file where embedding is allowed (e.g. PDF, XML formats), or separately such that the information file corresponding to the signature can be easily identified to facilitate verification by an independent person.

e) All information, including any supporting documents, stored and preserved by NeSL must be linked to clearly identifiable unique records of information (e.g. UDI) or person.

f) No financial information stored with NeSL shall be deleted or modified. Any update to information will be added as a new information record. All old records shall be preserved till purged after the specified period of time.

g) If and when permitted by the Regulatory standards or notification, NeSL may be allowed to store reference links to external registries (e.g. CERSAI) to enable IUs to fetch and retrieve related records/ documents on need basis to service user requests of information retrieval, without the need to import and replicate the entire database of such registries.

h) Similarly, for servicing any information requests related to information stored at other IUs, NeSL can retrieve such information on need basis as per the allowed norms of interoperability of IUs.

i) NeSL shall maintain and preserve audit trail of all usage of information, including submission, authentication and information retrieval activities for each user:

i. Minimum information to be maintained as audit trail for financial information shall cover at least the user ID, date and time, type of service used and record ID.
ii. In addition, NeSL shall maintain audit trail of other non-financial information such as user administration/ system access e.g. user creation, deletion, activation, change of user access privileges, change in user profiles including upload of DSC, login, session duration, unsuccessful login attempt etc.

j) NeSL shall maintain a backup of all financial information stored with them periodically in offline media storage to guard against possible data corruption of online storage/ servers:
   i. Such media storage shall be preserved in a secured manner to prevent unauthorized access or damage.
   ii. NeSL shall carry out periodic verification to check that the data on the media restorable.

k) In line with the generally accepted period of storage of public documents i.e. 5 to 8 years, NeSL shall preserve old records for a period of 8 years from the date of closure of loan:
   i. Considering that NeSL will not maintain a loan account with its status in a way the creditor does and that information maintained about a loan is in the form of a series of updates, each appended as new record, a closure of loan in this context will imply records of debt which have stopped receiving any updates.
   ii. NeSL shall preserve the records for 8 years from the date of reporting of closure of Loan account or date of last update
   iii. NeSL shall maintain a metadata about the purged records including UDI, creditor ID, debtor ID, other party IDs, last update date and date of purging.

CHAPTER – XIII

13. COMMITTEES

a) Subject to the provisions of the Companies Act, 2013 and Articles of Association of the Company, the Governing Board of NeSL may delegate, from time to time, to any committee or committees comprising of two or more directors, any of the powers vested in it upon such terms and conditions as it may think fit. It may cancel, withdraw, alter or vary all or any of such powers so delegated. The Governing Board of NeSL may at any time in its sole discretion remove any director on such committee or committees or modify the constitution thereof.

b) Without prejudice to the generality of the foregoing, the Board of Directors may constitute the following committee for compliance purposes:

i. Grievance Redressal Committee

NeSL has constituted the Grievance Redressal Committee to resolve any grievances referred to, as per the Grievance Redressal Policy. The Governing Board of NeSL will monitor and resolve any unresolved issues in respect of grievances addressed to grievance redressal committee.

ii. Compliance Officer

A Compliance Officer shall be appointed by NeSL who shall be responsible for ensuring compliance with the provisions of the Code applicable to the IU, in letter and spirit. The compliance officer shall, immediately and independently, report to the Board any non-compliance of any provision of the Code observed by him. The compliance officer shall submit a compliance certificate to the Board annually, verifying that NeSL has complied with the requirements of the Code, and has redressed customer grievances.

CHAPTER – XIV

14. RIGHTS & OBLIGATIONS OF USERS

Rights:

Users have a right to:

a) Know the terms and conditions governing the services offered by NeSL which shall be made available on the webpage of NeSL and easily accessible.

b) Receive open, clear and timely information about services including any fee payable, in a way that is understandable to them.

c) Receive services without any discrimination or harassment with all normal courtesy expected of a professional Institution.

d) Receive services based on their explicit consent.

e) Have their privacy protected and information submitted by them to be kept in strictest confidence.

f) Lodge grievance with NeSL through its website and a quick redressal of the grievances.

g) Request and gain access to the information submitted to NeSL according to the regulations in force.

h) Authorise, a third party to access the information relating to them.

i) Receive, free of charge an annual statement of all information pertaining to them.

j) Access information submitted to NeSL through any other Information utility.

k) Permit to view the date on which the information was last updated and also the status of authentication.

l) Port, the information submitted to NeSL, to any other Information utility without any hindrance.

Obligations:

a) The user shall, at all times, adhere to the Bye-Laws, Terms and Conditions of use of the NeSL services and the Privacy Policy in its dealings with NeSL.

b) The user shall at all times maintain the secrecy of its user account credentials in a safe and secure manner and NeSL shall not be responsible for any unauthorised use of the user account credentials.

c) By using the services of NeSL, the user represents and warrants that it is authorised to avail the services of NeSL through the user account it uses to access the same.

d) The user indemnifies NeSL and all its employees, representatives and/ or agents against any claim, loss, harm, liability or legal proceeding arising out of, or in connection with any unauthorised use of the user account.

e) The user shall ensure that the information submitted by it is true and correct.

f) The user shall update the information as expeditiously as possible.

g) The user shall pay the prescribed fee in advance or as agreed upon between user and NeSL.

h) The user shall not submit information other than that is required under the IBC.

CHAPTER – XV

15. GRIEVANCE REDRESSAL

a) A Grievance Redressal Policy shall be approved by the Governing Board of NeSL and the same shall be placed in the website of NeSL detailing the process of registering grievances, format for the same and the escalation matrix, if the grievances remain unresolved or the user is not satisfied with the resolution within a reasonable time.

b) The Grievance Redressal Policy shall provide for:

i. The Constitution of a Grievance Redressal Committee consisting of 3 senior managerial personnel and approved by the Governing Board of NeSL shall be formed.
ii. The functions of the Grievance Redressal Committee.
iii. The format and manner for filing grievances.
iv. Maximum time and format for acknowledging receipt of a grievance
v. Maximum time for the disposal of the grievance by way of dismissal.
vi. Details of the mediation mechanism.
vii. Provision of a report of the grievance and mediation proceedings to the parties to the grievance upon dismissal or resolution of the grievance.
viii. Action to be taken in case of malicious or false complaints.
ix. Maintenance of a register of grievances received and resolutions arrived at in respect of its services.
x. Disclosure of receipt and disposal of grievances to the public in the form and manner directed by the Board.
xi. Periodic reporting of the receipt and disposal of grievances to the Governing Board.
xii. Periodic review of the Grievance Redressal Mechanism by the Governing Board.

CHAPTER – XVI

16. DUTIES AND RIGHTS OF NeSL

Duties of NeSL:

NeSL shall –

a) Hold the information submitted to it by the submitters as a custodian and shall provide services with due and reasonable care, skill and diligence.

b) Provide services without discrimination in any manner.

c) Provide services to a user based on its explicit consent.

d) Guarantee protection of the rights of users.

e) Establish adequate procedures and processes and facilities to ensure that its records are protected against loss or destruction.

f) Adopt secure systems for information flows.

g) Protect its data processing systems against unauthorized access, alteration, destruction; disclosure or dissemination of information.

h) Transfer all the information submitted by a user, and stored with it to another information utility on the written request of the user.

i) Accept from an IP, reports, registers and minutes in respect of any insolvency resolution, liquidation or bankruptcy proceedings.

j) Make adequate arrangements, including insurance, for indemnifying the users for losses that may be caused to them by any wrongful act, negligence or default of NeSL, its employees or any other person whose services are used for the provision of services under these Regulations.

k) NeSL shall not –
    i. Outsource the provision of core services to a third-party service provider
    ii. Use the information stored with it for any purpose other than providing services under these Regulations, without the prior approval of the Board;

iii. Seek data or details of users except as required for the provision of the services under these Regulations.

Rights of NeSL:

NeSL shall –

a) Charge appropriate fee for the various services it offers.

b) Refuse registration of user if the ID verification fails or dedupe fails.

c) Refuse services if it finds that the NeSL's portal is used by the user for unauthorized purposes.

d) Import information from such registries as may be notified by the IBBI from time to time.

e) Amend the bye-laws and terms and conditions and change the fee structure from time to time after approval from appropriate authorities; the same will be notified to the users before implementation of the same.

Duties of NeSL:

a) Charge uniform fee for providing the same service to different users.

b) Disclose the fee structure for provision of services on its website.

c) Disclose any proposed increase in the fees for the provision of services on its website at least three months before the increase in fees is effected.

d) Ensure the fee charged for providing services is a reasonable reflection of the service provided, and providing access to information shall not exceed the fee charged for submission of information to the information utility.

CHAPTER – XVII

17. MISCELLANEOUS

a) An approved Exit management plan shall be put in place as required by Regulations which shall not be amended without the prior approval of the IBBI.

b) A preservation policy consistent with the technical standards providing for the form, manner and duration of preservation of information stored with NeSL and details of the transactions of NeSL with each user in respect of the information stored with it is in place is maintained to benefit early retrieval.

c) NeSL shall provide a functionality to access information stored with another IU as per the standards set for inter-operability between IUs.

d) Adequate security measures shall be built into such functionality to protect the privacy and confidentiality of information.

e) NeSL shall not be responsible for system failures or disruption of service in another IU due to which inter-operability is temporarily not feasible.

f) NeSL shall transfer all the information submitted by a user to another IU on the request of the submitter.

g) NeSL shall provide every user an annual statement of all information pertaining to that user stored by it, free of charge.

h) NeSL shall deny registering a user if the verification of ID of the user fails. The user shall be informed of the denial of service.

i) The user shall pay the fee promptly and on non-payment of fee, NeSL can deny further service.

j) Unauthorised access or unauthorised use of information is subject to civil, criminal, administrative, or other lawful action.