# GUIDELINES FOR TECHNICAL STANDARDS

# FOR THE PERFORMANCE OF CORE SERVICES AND OTHER SERVICES UNDER THE INSOLVENCY AND BANKRUPTCY BOARD OF INDIA (INFORMATION UTILITIES) REGULATIONS, 2017

**INSOLVENCY AND BANKRUPTCY BOARD OF INDIA**

**NEW DELHI**

## Table of Contents

# 1. Background

## 1.1 Scope and Objective

In exercise of the powers conferred by sections 196 read with section 240 of the Insolvency and Bankruptcy Code, 2016 (31 of 2016), the Insolvency and Bankruptcy Board of India (IBBI) notified the IBBI (Information Utilities) Regulations, 2017 which seek to provide a framework for registration and regulation of information utilities.

Regulation 13 under Chapter IV of the IBBI (Information Utilities) Regulations, 2017 provides that the Board may lay down Technical Standards through guidelines for the performance of core services and other services under the said Regulations. The Technical Committee constituted by IBBI on May 3, 2016 under the IBBI **(**Information Utilities**)** Regulations, 2017 under the chairmanship of Dr**.** R**.** B**.** Barman, submitted its first report on 16th August, 2017**.** This report has made recommendations on 14 out of 18 matters for which technical standards are required to be laid down by IBBI through Guidelines issued under the Regulations**.** Technical Standard related to remaining four topics under Regulation 13 will be laid down separately. The Technical Standards will ensure and enforce the reliability, confidentiality and security of financial information to be stored by the information utilities**.** In furtherance thereof, the Board hereby lays down Technical Standards on the basis of the recommendations given by the Technical Committee on Information Utilities.

The Technical Committee consciously did not prescribe any specific choice of technology or platform, so that each IU can exercise its own choice. Instead, it recommended that the IUs adopt robust data governance standards to take care of complete integrity of the IU database. In order that a single version of truth can be established, there should be unfettered access to data among the IUs, while each IU is free to maintain its own repository of mutually exclusive and exhaustive data.

The Technical Standards cover the following matters in accordance with Regulation 13 of the IBBI (Information Utilities) Regulations, 2017: -

a. standard terms of service;
b. registration of users;
c. unique identifier for each record and each user;
d. submission of information;
e. identification and verification of persons;
f. authentication of information;
g. verification of information;

h. data integrity;
i. consent framework for providing access to information to third parties;
j. security of the system;
k. security of information;
l. risk management framework;
m. preservation of information; and
n. purging of information.

In terms of the IBBI (Information Utilities) Regulations, 2017, an Information Utility shall ensure compliance with these Technical Standards at all times. Terms used in these Technical Standard Guidelines shall have the same meaning as assigned in the Insolvency and Bankruptcy Code, 2016 and the IBBI (Information Utilities) Regulations, 2017

## 1.2 ABBREVIATIONS

| | |
|---|---|
| API | Application Programming Interface |
| BCP | Business Continuity Plan |
| CERSAI | Central Registry of Securitisation Asset Reconstruction and Security Interest of India |
| CISA | Certified Information Systems Auditor |
| CERT-IN | Computer Emergency Response Team |
| CIN | Company Identification Number |
| DR Facilities | Disaster Recovery Facilities |
| DSC | Digital Signature Certificate |
| FC | Financial Creditors |
| IRP | Insolvency Resolution Professional |
| IBBI | Insolvency and Bankruptcy Board of India |
| IT Act | Information Technology Act, 2008 |
| IU | Information Utility |
| LLPIN | LLP Identification Number |
| MCA | Ministry of Corporate Affairs |
| OC | Operational Creditors |
| OTP | One-Time Password |
| ROC | Registrar of Companies |
| RPO | Recovery Point Objective |
| RTO | Recovery Time Objective |
| SOAP | Simple Object Access Protocol |
| UDI | Unique Debt Identifier Number |
| UIN | Unique Identification Number |
| UIDAI | Unique Identification Authority of India |

## 2.1 REGISTRATION, IDENTIFICATION AND VERIFICATION OF USER (Regulation 13(2)(c) and Regulation 13(2)(f))

The Technical Standards for the registration of users and for identification and verification of persons shall be governed by the following key objectives:

A. The Registration of any User shall be undertaken by an IU before any service is provided.

B. The Identity of a User shall be verified based on a single primary identifier type. The access control shall ensure that the user is uniquely identified by the primary identifier that is issued by a government authority. Multiple types of ID options shall not be used for the same category of Users.

C. The extent of verification of the Identifier taken from the User by the IU, shall determine the quality of evidence that shall attach to the authentication process which is facilitated by the IU.

D. The Registered list of Users and their UINs shall be shared by the IU with others IUs.

E. The digital signatures, as defined under the Information Technology Act and in a permitted form such as through traditional digital signature certificates or Aadhaar based e-sign, are at the core of the IU processes and a directory of digital signature certificates (where traditional digital signature is opted for) shall be maintained by an IU as part of registered user data for future reference or validation.

F. An IU shall monitor the registration and user administration activities.

### TECHNICAL STANDARDS 13(2) (c) and 13(2) (f)

1. An Information Utility shall undertake the following processes for Registration, Identification and Verification of Users:

   a) Capture the minimum required information as specified in these guidelines covering identity and contact details;

   b) Conduct a de-duplication check across all IUs to ensure that the User is not already registered;

   c) Verify the identity of the User against the original issuer of ID;

   d) Upload the Digital Signature Certificate (if available) and its verification with the certifying authorities;

   e) Receive an acceptance from the User, of the terms of usage as formulated by the concerned Information Utility;

   f) Receive the fees as published by the IU on its website;

g) Allot the Unique Identifier Number (UIN – described under the Technical Standards pertaining to Unique identifier for each record and each user at 2.2)

h) Issue the user ID and password to the User

2. **Individual persons** seeking registration, shall provide only their Aadhaar ID at the time of availing the services of an IU

   a) The Aadhaar based process shall apply to all Indian residents and to any other individual persons holding Aadhaar.

   b) The IUs shall conduct a de-duplication to check if the same Aadhaar Number has already been used previously in the same IU or any other IU.

      i) In case a match is found, i.e., where the person has earlier verified his/her credentials, the IU shall perform an identity verification against the UIDAI database. This process shall require a mobile based OTP confirmation or a biometric verification of the credentials.

      ii) In case no match is found, the IU shall verify the identity against the UIDAI database and also capture other related demographic particulars, including date of birth, address, mobile number, email ID as per UIDAI records and use the same for internally creating a registration record automatically.

   c) No user ID/ password needs to be issued to individual person with Aadhaar.

   d) For non-resident Indians or foreign individuals, IUs should provide alternative mechanism to accept other supporting documentation.

3. For a **legal entity seeking registration,**

   a) An IU 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:

      i) Name of entity

      ii) Type of person/ Legal constitution (e.g. Company, LLP, Partnership, HUF, Society etc.)

      iii) Indian/ Overseas status

      iv) PAN as the primary ID

      v) CIN/ LLPIN (if registered with MCA)

      vi) Date of incorporation

      vii) Representative person's full name

      viii) Representative's designation

      ix) Aadhaar ID for the representative or alternative verification through PAN

x) Primary Email ID

xi) Alternative Email ID

xii) Primary Mobile number

xiii) Alternative Mobile number

xiv) Landline number (if available)

xv) Registered office address with PIN Code

xvi) Communication/ billing address with PIN Code

b) An IU 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.

i) If a match is found, the user shall be informed and asked to login.

ii) If the de-duplication returns 'not match', the IU shall verify the PAN with the issuing authority (IT Department database).

iii) For the legal entity's authorised representative, the Aadhaar ID shall be cross-checked with UIDAI through OTP/biometric process. Alternatively, verification of his/her PAN ID along with digital signature certificate will be performed.

c) As a part 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. 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:

i) In case of a legal entity, the IU shall verify such DSC, when submitted, to check its validity.

ii) In addition, the IU shall check if the name of the legal entity, as per the registration data matches the name of the organisation in the DSC, if included in the DSC. The name of the authorised representative as provided for in the DSC should also be cross-checked against his Aadhaar ID.

iii) In case the name of organisation and the representative have been cross-checked in terms of point (ii) above, no further supporting documentation shall be required and the registration process can commence.

iv) 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 the IU in order to confirm that the person being registered is authorised to represent the legal entity. In case of an authorisation based on a Power of Attorney, the authorization shall be checked against the Resolution of the

Board. In such a situation, the IU shall be required to check the contents of the Board Resolution and then approve the registration request.

v) **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. The IU systems should use only verified contact information. No verification of postal address is required to be performed by the IU.

4. Before the completion of registration, the person being registered must accept the **terms of usage** as specified by the IU. This shall also apply to individuals accessing through Aadhaar validation.

5. Registration process shall be completed with PAN (legal entity) or Aadhaar (individual) being treated as the **Unique Identification Number (UIN)**. In case of non-resident Indians or foreign nationals, a UIN shall be issued by the IU.

6. The IU shall send a **confirmation email** on the completion of the registration process. IUs 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 the IU portal for the first time, he/she shall need to provide a second factor as credential in the form of date of incorporation and shall be required to change the password on first use.

7. The authorised representative of the legal entity can access all IU 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 IU 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. The IU is not required to verify the identity of any additional users created under the authority of the registered authorised representative of the entity.

8. 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.

9. The IU should 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. This and other surveillance mechanisms have been addressed under the Technical Standards pertaining to Security of System and Security of Information at Point 2.7

## 2.2 UNIQUE IDENTIFIER
## (Regulation 13(2)(d))

The technical standards for unique identifier for record and each user are governed by the following aspects:

1. The allotment of Unique Identifier to a User shall be undertaken by an IU after completion of the Registration Process.
2. For allotment of Unique User Identifier Number (UIN), the technical standards are based on the primary identifiers i.e. PAN or Aadhaar Number.
3. For allotment of Unique Debt Identifier Number (UDI), the technical standards are based on the combination of Loan Account Number allotted by the Creditor plus UIN of the Creditor (e.g. PAN), thereby making it unique.
4. The information utility shall create and maintain appropriate list of Registered Users, the Unique Identifiers of Registered Users and the Unique Identifiers assigned to the Debts.
5. The IU shall ensure that the lists created as above, are available to all Information Utilities and the IBBI.

### Technical Standards on Regulation 13(2)(d)

**Unique Identifier Number to Users (UIN)**

1. Aadhaar Number for individual users and PAN number for all legal entities shall be directly used as UIN. Depending on the type of person, the PAN or Aadhaar field shall be used as the identifier.
2. The Unique Identifiers are as under:
    - For Individual Users (Aadhaar Number) (12 Digits): ex. **469485907737**
    - For Legal Entity: (PAN Number) (10 Digits): ex. **AADPU6217E**
3. 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 IU in their respective systems. All systems at the creditors' end will already have provisions for PAN and Aadhaar fields. Hence, implementation of IU interface will be easier. Further, even users do not need to remember any new number assigned to them.
4. For non-resident Indian individuals or foreign nationals/entities, not covered by Aadhaar or PAN, IUs shall assign a new number since no fixed document type is applicable. The UIN in such case shall be a serial number issued by the IU, starting with IU code (1 digit), single digit indicator for type of person, followed by a 10-digit serial number e.g.

- For non-resident/foreign individuals: 110000000023 (1 for IU code, 1 for Individual and serial number 23)
- For overseas entity: 120000000009 (1 for IU code, 2 for legal entity and serial number 9.

**Unique Debt Identifier (UDI)**

5. 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 or Aadhaar) is necessary for uniqueness of UDI since it is possible that two creditors may have issued the same loan number.
6. 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 Aadhaar ID (12 digit) will be UIN. To ensure that loan number can be easily derived from the UDI, in case PAN number is applicable as UIN, two digits of 00 will be inserted after PAN and before loan account number so that loan number always starts from 13$^{th}$ digit of UDI.
7. UDI (total digits 32 max) will reflect as follows:
    - If PAN is AADPU6217E and loan a/c no is 12345678900987654321, UDI will be **AADPU6217E0012345678900987654321**
    - In case of individual creditor with Aadhaar no 469485907737 and loan number of HP/01283/2017-18, the UDI will be **469485907737HP/01283/2017-18**
8. The key advantage of this approach is that the loan number as existing with the creditor is retained and no new number is introduced. De-duplication check for new loan record is also easier since the UDI list is shared across IUs and knowledge of just the UDI is sufficient to run deduplication.

## 2.3 SUBMISSION OF INFORMATION
## (Regulation 13(2)(e))

The Technical Standards for submission of information cover the following:

1. The submission of information in an Information Utility shall be done with the digital signature of the submitter
2. All Form C data, except default reporting, for a debt shall be submitted in one file. A single submission file may have data about multiple debts.
3. The updated data submission shall be in the format of Form C.
4. Supporting documents to a debt or security can be submitted for a debt separately at any time.
5. Default can be reported at any time by the creditor in Form C.
6. Submission of balance sheet/ cash-flow statement and also submissions by IRP shall be done at the debtor level.
7. Any error, if comes to the notice, can be marked erroneous by the submitting party only.
8. An acknowledgement is to be issued to the submitting party on receipt of any submission of data/ document.

### Technical Standards on Regulation 13(2)(e)

1) Any information submission, whether in data format or as a document, shall be **digitally signed** by the submitter. The Digital signature should be of requisite class as specified in the standards for security of information. Individual submitter can opt for Aadhaar based e-sign.
2) Submission of debt related data shall be made together in the **same file** i.e. submitter identity, related party information and security information is to be part of the same file containing the debt information which also includes outstanding liabilities:
   a) The format for such submission will as per **Form C placed as annexure** or with modifications as needed by IU**,**
   b) 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
   c) 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.
   d) The section on default (Form C in Annexure) will not be part of the regular debt data submission but will be undertaken only at the time of reporting of default.
3) Submission of supporting documents: Documents can be submitted at any time, not necessarily along with Form C data submission. Such documents should support multiple formats including PDF and scanned image files. All document submissions must also be digitally signed by the submitter:
   a) Each supporting document for debt shall have a debt unique identifier reference

b) Each supporting document for security shall have security identifier reference, which will be the CERSAI ID.

4) Default reporting: creditor may report default of a debt with reference to a specific debt. For reporting of default:
   a) Data as per section on Default in Form C will be submitted
   b) Creditor may upload/ submit any supporting documents as proof of default along with the data of default
5) Submission of balance sheet & cash flow statement: the debtor or its authorised Auditor can submit audited balance sheet and cash-flow statements as electronic documents (PDF, scanned documents etc.)
   a) This shall be submitted with reference to debtor unique identifier (i.e. PAN)
   b) Such submissions can be made directly to the IU
   c) Alternatively, IU may consider porting such statements already submitted by the debtor or its Auditor to MCA in digitally signed mode, thereby avoiding the need for direct submission to IU
6) Submission of other information by IRP
   a) The IRP must be a registered person like any other submitter of information
   b) The IU shall check that the IRP has a valid registration number issued by IBBI. This should be validated using an API provided by IBBI.
   c) Based on court order documentation made available to IU, the IU will 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 the IU.
   d) All submissions of IRP will be with reference to debtor unique identifier
   e) 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.
7) IUs 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 SOAP based API service or push from creditor's server to a designated SFTP server) or even screen based entry of one record at a time.
8) 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.
9) Exception handling: submitted information will be rejected by IU if
   a) One or more records of a bulk submission file are found not conforming to the specified format or missing mandatory fields
   b) Digital signature is found missing, invalid or expired
10) Error-correction: 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.

11) Issuing of acknowledgement:
    a) 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.
    b) The acknowledgement should specify key information submitted, including receipt date, unique identifier allotted by IU as applicable, terms & conditions of authentication and verification. The terms and conditions for authentication and verification should contain IU's plans and means of approaching the concerned parties for obtaining authentication.
    c) All information utilities shall ensure that the submitting user is able to download, if needed, the acknowledgement as a PDF digitally signed by IU, at any point of time.

## 2.4 AUTHENTICATION AND VERIFICATION OF INFORMATION (Regulation 13(2)(g) and 13(2)(h))

The standards for authentication and verification for information are governed by the following aspects:

1. Facilitating authentication of information from all concerned parties is a core function of an IU.
2. IU 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.
3. IU shall maintain status of authentication for each record of information including any dispute
4. IU should preserve each artefact used during submission and authentication in its original form as used during digital signature, for the purpose of checking veracity at any time.
5. On authentication of default, IU should inform all related parties to the debt and also all creditors related to the debtor.

### Technical Standards on Regulation 13(2)(g) & 13(2)(h)

1. When a link for authentication is presented by an IU, 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 Aadhaar credentials.
2. Any registered user, on logging into/ accessing the IU portal, shall be presented with all pending authentication requests in the relevant section of the portal.
3. The authentication page containing the information will be displayed by the IU to the authenticating person only after verifying identity and credentials of the person from the registration information, whether registered with the same or a different IU.
4. IU 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.
5. When the authenticating party confirms the information and digitally signs the same, IUs must ensure that the digital signature is based on and affixed to an artefact (data file/ document) with the same version of the information presented to the authenticating party for verification:
    a. For users representing a legal entity, such user is expected to use digital signature certificate (DSC) that has been registered with the IU 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.

b. 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.

6. IUs must 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.

7. When the authenticating party disagrees with or disputes a part of or entire information presented, IUs shall provide for obtaining reasons for dispute. 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. IU 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.

8. If the authentication request, sent to the concerned party, remains unauthenticated beyond 7 days, the authentication will be considered having 'failed authentication' and the same record will not be available for authentication by the same party subsequently.

9. The different 'status' of authentication which needs to be maintained by an IU for each record and each party shall cover:

    a. '*To be 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.

    b. '*Pending authentication*': when the concerned party is yet to undertake authentication.

    c. '*Failed authentication':* if the specified time limit of 7 days is exceeded

    d. '*Authenticated':* when the concerned party verifies, agrees to the information presented and affixes his/her digital signature (or e-Signs) to the information as presented without any change.

    e. '*Disputed':* when the concerned party disagrees/disputes a part of or the entire information presented for authentication

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

11. If submitted information of default is authenticated by the concerned party or by any third party through any standard mechanism as notified by the Regulator from time to time, IUs shall send a default confirmation alert to the following along with information of the debt and the debtor:

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

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

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

## 2.5 STANDARD TERMS OF SERVICE
## (Regulation 13(2)(b))

The standards for authentication and verification of information are governed by the following aspects:

1) IUs shall provide the services without discrimination between users.
2) IUs shall not deny services to any person on the basis of place of residence or business or type of personality.
3) IUs shall provide qualitative and error free services to its Users.
4) The terms and conditions covering the services and fee structure for its various services shall be informed by the IU upfront to the user and also displayed on its website.
5) IUs shall charge uniform fee for providing the same service to different users.
6) Any change in the fee structure of an IU shall be notified to the user atleast 3 months before the effective implementation date.
7) IUs shall put in place suitable Grievances Redressal Mechanism operated on an electronic platform and ensure prompt redressal of grievances.
8) IUs shall provide services to a user based on its explicit consent.

### A. User Registration

1) IUs shall verify the Identity of the users registering with it.
2) On registration, the users shall be given a Unique ID and the same shall be communicated by email to the Users by the IU
3) IUs shall do a deduplication with other IUs and within its database and can deny registration if the user is already registered

### B. Submission of Information

1) All information submitted in an IU shall be through electronic mode only.
2) The format for capturing the information may include the details as required under Form C or with modifications as required by the IU.
3) On receipt of information submitted by the user and on authentication, the IU shall send an acknowledgement to the user of receipt of the information with specific ID numbers of the Debt / Record
4) Only the original submitters of information shall be allowed to mark erroneous records.
5) IUs 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 and deny storing of any other information not related to the above

### C. Authentication of Information:

1) IUs shall facilitate the authentication of information through electronic mode duly ensuring that the data is sent to the authorised persons only

2) IUs shall stipulate authentication of information by the Users by using Digital Signature Certificates/e-Sign.
3) IUs shall provide the status of information to the submitter of the information;
4) All other users connected to the debt shall also be permitted to view the status of authentication
5) IUs shall take reasonable care in identifying the persons authenticating the information

**D. Storage and Access to Information:**

1) The financial information collected by the IU shall be stored securely, duly ensuring adequate safeguards and security as prescribed in the Information Technology Act, 2000
2) Access to data shall be provided only to authorised persons after verifying their identity through log-in credentials
3) Suitable Business Continuity Plan & Disaster Recovery Mechanisms shall be put in place by the IU.
4) Appropriate Security Audits shall be ensured by the Information Utility periodically.

**E. Others**

1) IUs shall provide a functionality to access information stored with another IU as per the standards set for inter-operability between IUs.
2) Adequate security measures shall be built into such functionality to protect the privacy and confidentiality of information.
3) IUs shall not be responsible for system failures or disruption of service in another IU due to which inter-operability is temporarily not feasible.
4) IUs shall transfer all the information submitted by a user to another IU on the request of the submitter.
5) IUs shall provide every user an annual statement of all information pertaining to that user stored by it, free of charge.
6) IUs shall deny registering a user if the verification of ID of the user fails. The user shall be informed of the denial of service.
7) The user shall pay the fee promptly and on non-payment of fee, IU can deny further service.
8) Unauthorised access or unauthorised use of information is subject to civil, criminal, administrative, or other lawful action.

## 2.6 CONSENT FRAMEWORK
## (Regulation 13(2)(j))

**The Technical Standards for the consent framework for providing access to information to third parties are as follows:**

1. For **individuals,** the consent artefact shall capture the following details:
    - Primary Identifier of the individual to whom the consent is provided
    - Name (as Per Aadhaar)
    - Start date of authorisation
    - End date of authorisation
    - Reason for authorisation
    - Consent for Debt Id: Values could be 'ALL' or 'specific' debt numbers (comma separated if multiple debts)
2. For **legal entities**, the consent artefact shall capture the following details:
    - Primary Identifier of the representative to whom the consent is provided
    - Name (as per the Primary Identifier)
    - Start date of authorisation
    - End date of authorisation
    - Reason for authorisation
    - Consent for Debt Id: Values could be 'ALL' or 'specific' debt numbers (comma separated if multiple debts)

For further details, the MeitY framework document can be obtained from the following link: http://dla.gov.in/sites/default/files/pdf/MeitY-Consent-Tech-Framework%20v1.1.pdf

## 2.7 DATA INTEGRITY AND SECURITY
## (Regulation 13(2)(i), 13(2)(k) and 13(2)(l))

The technical standards relating to data integrity and security of system and information address the following aspects:

1. IT security policy and Cybersecurity policy, detailing all preventive measures to mitigate data security risks, is to be put in place
2. The data center and disaster recovery design and operations should conform to performance standards and operational standards
3. For security standards, IUs should consider relevant security frameworks (including cybersecurity) used by regulatory bodies like RBI and SEBI. IUs should consider Information Security standards such as ISO 27000 for adoption.
4. Business Continuity Plan document of IU should be approved by IBBI
5. IUs should establish a robust capacity planning policy
6. Regular security and software audits by 'Cert-in certified auditors' should be conducted
7. 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
8. Building resilience in every sphere of IT function viz., system development, testing, deployment, production, monitoring, etc., with formal review process to mitigate hidden risks
9. Role and reporting segregation between Chief Technology Officer and Chief Information Security Officer to avoid conflict of interest

### Technical Standards on Regulations 13(2)(i), 13(2)(k) & 13(2)(l)

**Information Availability:**

1. The IUs data center and Disaster Recovery design and operations should conform to performance standards, such as Uptime Institute's Tier Standards with a data center rating of Tier 3 or above. IU service shall be hosted in a data center and DR facilities shall be within India and be governed by its applicable laws.
2. Business continuity of IT systems should be ensured through Disaster recovery (DR). IUs should 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 should be adequate considering the nature of IU activity. The same should be reviewed periodically by the IU.
3. A set of policies and procedures should be adopted to enable the recovery or continuation of service following a natural, human-induced disaster or any technological issues
4. 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.
5. IUs should put in place a robust capacity planning policy.

**Information Confidentiality:**

1. IU service shall conform to security standard certification such as ISO 27001. IU should consider adopting security frameworks (including cybersecurity) used in regulatory bodies such as RBI and SEBI. Such standards should be put in place in a graduated manner over next two years or as directed by IBBI.
2. The data should be transferred using secure, authenticated and industry-accepted encryption mechanisms to avoid malicious users intercepting the data and gaining unauthorized access
3. IU should establish adequate security systems to protect the data processing systems against unauthorised access, alteration, destruction, disclosure of information. Encryption of stored data may be restricted to more sensitive columns
4. Suitable access control measures to be put in place to prevent unauthorised access to any internal or external persons
5. The Data Centre and DR design should 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.
6. Since application is exposed to internet, application security testing should be ensured. Application should be tested for security vulnerability. Secure coding standards must be enforced to ensure that such vulnerabilities are not created in the first place and audit of the code should be undertaken to ensure the same.
7. Adherence to the best security practices, with regular security audits by enlisted auditing firms that may be empanelled or that conform to some minimum standards. IU should submit reports of system and IS audit to IBBI.
8. Secure data access should be enabled through *sftp* for bulk transfer and *https* for browser based access
9. Network security should be enforced using Firewall, Intrusion Detection/Protection System, Anti-bot, Antivirus/ Anti malware/ Anti-Spam

**Information Integrity:**

1. Change Management policies for software releases shall be enforced
2. Verify the identity of the person registering through generally accepted, easily verifiable and reliable sources such as Aadhaar, PAN ID issued by government agencies before allowing the registration. Before registering a user, IUs shall ensure that the same user is not registered in any other IU.
3. Email address and mobile number shall be verified.
4. Validation of the record of debt in the system of IUs to ensure that every debt record is unique before it is stored in an IU.
5. IUs shall accept only digitally signed data/information from the submitter. The digital signature shall be Class 2 or above
6. All information artefacts (data/documents) submitted to the IU shall be stored in the original form for any future reference or verification
7. IU systems should maintain Audit Trail of users, such as IP address, date and time of access

## 2.8 RISK MANAGEMENT
## (Regulation 13(2)(m))

**Regulatory Context**

1. The Regulations expect the IUs to put in place robust risk management mechanisms to manage the risks embedded in the operations of the IU

2. Regulation 13 states that the Board may lay down standards, through guidelines, for different matters which are all pointers towards risk management.

3. Regulation 15 mandates every IU to have bye-laws consistent with the Code and inter-alia providing for risk management.

4. 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)

**Key considerations**

Operational Risk revolves around People, Processes & Technology. Yet in a technology based entity like an IU the emphasis is expectedly more on the risks revolving around the IT systems.

The risk management framework should:

1. Define processes to identify, assess, and manage all the risks that may affect the activities of the IU;
2. Encourage high level of accountability across the organisation;
3. Put in place open and transparent communication across the entire organisation; and
4. Clearly identify persons responsible for managing the risk and controls in place.

### Technical Standards for Regulation 13(2)(m)

1. **Identification of risk**
   a. The objectives of the organisation have to be clearly stated
   b. All potential risks affecting the various operations/services should be identified.
   c. External factors affecting the objectives of the organisation like technological changes/ obsolescence, regulatory changes, risks embedded in outsourced services/vendors etc should be considered
   d. Internal risk factors at the organisational level including interruptions in IT systems, man-made or natural disasters affecting the operations shall be considered
   e. Employees should 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.

2. **Assessment of Risk**

a. Assess the identified risks as to what will be the impact if that risk has to occur through probability and impact study.
b. The risks have to be assessed based on the likelihood and impact on the objectives of the organisation
c. Impact of the risk on earnings, reputation, business and legal implications have to be assessed
d. Assessed risks may be rated as Low, Medium or High depending upon the probability and impact.

3. **Managing the risk**

a. Risks that cannot be shared, transferred or avoided shall be managed
b. Decision to share the risk to be decided e.g., through insurance cover.
c. A risk register to document various risks under People's risk, Operational or Process risk, IT risk, Compliance risk etc., may be prepared.
d. For managing People's Risk, an IU should initiate steps to enforce a culture of integrity & honesty, monitoring work, providing training/retraining for enhancing skills, etc.
e. For managing Process Risk, an IU should 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.
f. For managing Technology Risk, an IU should put in place:
    i. Reliable, recoverable and secure systems,
    ii. Robust Access Control Systems for Data Security,
    iii. Network intrusion prevention Systems,
    iv. Business Continuity Plans by establishing Disaster Recovery Centre/Near Data Centre,
    v. Getting the VAPT (Vulnerability and Penetration Testing) Tests done at periodical intervals,
    vi. Systems Audit done by CISA qualified external auditors on its IT Framework/interface,
    vii. Information Security Audit
    viii. Adopting Quality Standards and getting Quality Standards Certifications / ISO Standards Certifications etc.
g. Risk should be managed by persons close to the risk e.g. unit head, business head, CTO/CISO etc.
h. Controls should be tested on a periodic basis to ensure effectiveness of the controls
i. Findings of Audits to be placed before the Board of Directors of the IU which has the overall supervisory responsibility and ensures that proper risk management practices are implemented;

4. **Responsibility in risk management**

a. The CEO has the overall responsibility and ensures that every employee of the organisation is aware of risks affecting the operations

b. 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 should review the risk management process at regular intervals.

5. **Monitoring the risk management process**

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

b. The Regulatory committee may supervise the compliance risk and the external Auditor shall give its report to the Regulatory Committee.

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

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

## 2.9 PRESERVATION AND PURGING OF INFORMATION (Regulation 13(2)(q) and 13(2)(r))

### Technical Standards

1. All information maintained by an IU will be in electronic form only.
2. IU can 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.
3. Any artefact, in the form of data file or scanned /other documents, which are digitally signed by a user of an IU, 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.
4. 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.
5. All information, including any supporting documents, stored and preserved by IU must be linked to clearly identifiable unique records of information (e.g. UDI) or person.
6. No financial information stored in an IU 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.
7. If and when permitted by the Regulatory standards or notification, an IU may be allowed to store reference links to external registries (e.g. CERSAI) to enable IU 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.
8. Similarly, for servicing any information requests related to information stored at other IUs, an IU can retrieve such information on need basis as per allowed norms of inter-operability of IUs.
9. IU is required to 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 will cover at least the user ID, date and time, type of service used and record ID
    ii. In addition, IU should 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.
10. IUs shall maintain 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. IU should carry out periodic verification to check that the data on the media is restorable.

11. **Duration of preservation and Purging of data:** In line with the generally accepted period of storage of public documents i.e. 5 to 8 years, IUs shall preserve old records for a period of 8 years from the date of closure of loan:

    i. Considering that an IU 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. An IU may permanently delete records of debt where the last updation date is earlier than 8 years.

    iii. IU shall maintain a metadata about the purged records including UDI, creditor ID, debtor ID, other party IDs, last updation date and date of purging.

**********

## Annexure: Description of fields in Form C

### A - 1. Submitter Information

| Sl. No. | Field Name | Field Type | Description of the field | Form C (Reg) | Remarks |
|---|---|---|---|---|---|
| 1 | Submitter's Unique Identifier Number (UIN) allotted by IU | Text | PAN No. for legal entity & AADHAAR No. for individuals | Y | |
| 2 | Submitter's name | Text | Formal name (First +Middle+Last) without salutations | Y | |
| 3 | Relationship of submitter to the Debt | LoV | 'Creditor', 'Debtor' 'Guarantor' etc | Y | Will be 'Creditor' in most cases. But can be a 'Debtor' or 'Guarantor' in some situation |

| | | | | | |
|---|---|---|---|---|---|
| 4 | Date of Incorporation (Legal Entity) / Date of Birth (Individuals) | Date | As declared | Y | For registered submitter, will be picked from registration data. Need not be part of data file |
| 5 | Communication address of submitter | Text | | Y | For registered submitter, will be picked from registration data. Need not be part of data file |
| 6 | PIN code of submitter | LoV | Valid PIN code from list (communication) | Y | For registered submitter, will be picked from registration data. Need not be part of data file |

| Sl. No. | Field Name | Field Type | Description of the field | Form C (Reg) | Remarks |
|---|---|---|---|---|---|
| 7 | Telephone number | Text | With ISD country and STD area code | Y | For registered submitter, will be picked from registration data. Need not be part of data file |
| 8 | Mobile number | Text | With ISD country code | Y | For registered submitter, will be picked from registration data. Need not be part of data file |
| 9 | Email ID | Text | | Y | For registered submitter, will be picked from registration data. Need not be part of data file |

**A-2. Other Party Information** (Repeat field set for each party)

| Sl. No. | Field Name | Field Type | Description of the field | Form C (Reg) | Remarks |
|---|---|---|---|---|---|
| 10 | Relationship to debt | LoV | Debtor', 'Creditor', 'Guarantor' 'Co-applicant', Co-obligant' etc | Y | Other party to be different from the submitter. If submitter is creditor, other party cannot be a creditor |
| 11 | Counterpart y name | Text | As per submitter (First+Middle+Last without salutations) | Y | |
| 12 | Registered/ permanent Address of counterparty | Text | Registered office address for legal entity<br>Permanent address for Individuals | Y | |

| Sl. No. | Field Name | Field Type | Description of the field | Form C (Reg) | Remarks |
|---|---|---|---|---|---|
| 13 | PIN code (Regd. Office) | LoV | Valid PIN code from list (registered/ permanent) | Y | |
| 14 | Address for Communication | Text | Current Communication address | Y | |
| 15 | PIN code (Comm. Address) | LoV | Valid PIN code from list (communication) | Y | |
| 16 | Legal Constitution | LoV | Public Ltd Co/ Pvt Ltd Co / LLP / Partnership/OPC/Resident Individual/ Non-resident/Foreign | N | Needed for validation of type of ID to be checked |
| 17 | Date of Incorporation (Legal Entity) / Date of | Date | As declared | Y | |

| | | | | | |
|---|---|---|---|---|---|
| | Birth (Individuals) | | | | |
| **Sl. No.** | **Field Name** | **Field Type** | **Description of the field** | **Form C (Reg)** | **Remarks** |
| 18 | Corporate Identification Number (CIN/LLPIN) for Corporates | Text | For registered legal entities | N | For de-duplication |
| 19 | PAN No. | Text | For legal entity and also individuals. Mandatory for legal entity other than foreign | N | For identity/ de-duplication |
| 20 | AADHAAR | Text | Mandatory for resident individuals. | N | For identity/ de-duplication |

| | | | | | |
|---|---|---|---|---|---|
| 21 | Counterpart y Contact Person Name | Text | Contact of representative employee | N | Needed for reaching out for authentication |
| 22 | Contact Person’s Designation | Text | As per submitter | N | Needed for reaching out for authentication |
| 23 | Contact Person’s Mobile No. | Text | As per submitter. One of mobile or email mandatory | Y | Needed for reaching out for authentication |
| 24 | Alternative Mobile No. | Text | | N | |
| 25 | E mail id | Text | As per submitter (official email ID) | Y | Needed for reaching out for authentication |
| 26 | Alternative Email ID | Text | | N | |

## A-3. Debt Information

| Sl. No. | Field Name | Field Type | Description of the field | Form C (Reg) | Remarks |
|---|---|---|---|---|---|
| 27 | Loan A/c Number | Text | Contract No. for Bills /LC/ Bank Guarantees; & Loan No. for Term Loans and OD/CC (For OC: Invoice No.) | Y | Creditor's loan number, mapped with UDI at IU end |
| 28 | Old Account Number (wherever applicable) | Text | Link to the Old account number to maintain history Creditor's PAN (i.e UIN) + old Loan a/c number | N | Audit trail and migration related issues |
| 29 | Date of Sanction of Credit Facility | Date | Date of latest renewal for OD/CC limits & Date of sanction for Term Loans (For OC: Date of Invoice) | Y | |

| | | | | | |
|---|---|---|---|---|---|
| 30 | Date of disbursement or activation | Date | Date of first disbursement for OC: Date of delivery | Y | |
| 31 | Currency of loan or exposure | LoV | Applicable Currency Code (e.g. INR, USD) | Y | All amounts in other fields will be in this currency |
| 32 | Sanctioned Amount | Number | Amount sanctioned<br>For OC: Amount of Invoice<br>Non-funds based it is the sanctioned limit | Y | |
| 33 | Nature of credit facility | LoV | Category code for product - Financial (fund/ non-fund based), Operational, secured/unsecured | Y | |
| 34 | Facility name | Text | Free text of product name | N | As known to debtor. To be presented during authentication |

| | | | | | |
|---|---|---|---|---|---|
| 35 | Repayment frequency | LoV | Monthly, Quarterly, Half yearly, Annual, On demand, bullet, Rolling, Others | Y | Repayment schedule difficult to get from creditors as per feedback |
| 36 | Rate of interest | Number | Applicable rate of interest on date of reporting | Y | |
| 37 | Lending arrangement | LoV | Sole Banking / Consortium / MBA | N | To link with security and numbers of creditors |
| 39 | Total Outstanding Amount | Number | Total outstanding as on the date of reporting including Principal, Interest, Charges etc. (For Fund based Limits); For non-fund based limits, please indicate Contingent Liability; For OC: Amount due under the invoice | Y | |

| Sl. No. | Field Name | Field Type | Description of the field | Form C (Reg) | Remarks |
|---|---|---|---|---|---|
| 40 | Amount Overdue | Number | Amount overdue (aggregate of principal, interest, charges etc.) as on date of reporting | N | Data to be used for evidencing default<br>If no overdue, report zero value |
| 41 | Days past due (DPD) | Number | Number of days overdue as on date of reporting | N | DPD applicable across all creditors (non-banking, operational etc) - data to be used for evidencing default<br>If no overdue, report zero value |

**B. Security Information**

| Sl. No. | Field Name | Field Type | Description of the field | Form C (Reg) | Remarks |
|---|---|---|---|---|---|
| 42 | Date of creation of charge | Date | As stored by the Creditor | Y | Mandatory where security record submitted |
| 43 | Type of Charge created | LoV | Indicate whether it is: Mortgage / Hypothecation / Charge / Assignment / Pledge / Lien / Negative Lien | Y | Mandatory where security record submitted |

| | | | | | |
|---|---|---|---|---|---|
| 44 | Assets type | Text | Free text description of asset type over which charge created (Movable/ immovable/ intangible etc.) | Y | Mandatory where security record submitted<br>Illustrative list:<br>Cash / Bullion / Bank Deposits<br>NSCs/KVPs<br>LI Policies<br>Shares/Bonds/Securities<br>Inventory (Raw Materials, WIP & Finished Goods<br>Accounts Receivables<br>Other Current Assets (Indicate whether Raw Materials/Stocks in Process / Finished Goods; Book Debts etc.)<br>Plant & Machinery / Equipment<br>Land & Buildings<br>Vehicles<br>Other Fixed Assets<br>Other Movable Assets |

| Sl. No. | Field Name | Field Type | Description of the field | Form C (Reg) | Remarks |
|---|---|---|---|---|---|
| 46 | Description of security | Text | Any description or details like number, identification marks etc. | Y | To facilitate authentication of security. Other fields do not provide sufficient information to identify security |
| 47 | Value of security | Number | Value of asset over which charge is created | Y | Mandatory where security record submitted |
| 48 | Date of valuation | Number | Date of valuation report for immovable properties & Date of Stock Statement for Stocks & Book Debts | Y | Mandatory where security record submitted |

| | | | | | |
|---|---|---|---|---|---|
| 49 | Security Classification | LoV | Primary or collateral | Y | |
| 50 | Security Interest ID with ROC | | As available with the creditor | N | |
| 51 | Security Interest ID as per CERSAI | | As available with the creditor | Y | |

## C. Default Information

| Sl. No. | Field Name | Field Type | Description of the field | Form C (Reg) | Remarks |
|---|---|---|---|---|---|
| 52 | Loan A/c Number | Text | Loan account on which default is reported | Y | Creditor's loan number, mapped with UDI at IU end |
| 53 | Date of default | Date | Due date for payment; | Y | |
| 54 | Total Outstanding | Number | Total outstanding as on the date of reporting including Principal, Interest, Charges etc. | Y | |
| 55 | Default amount | Number | Amount fallen due but not paid | Y | |
| 56 | Days past due | Number | As on date of reporting default | Y | |
| 57 | Amount of last repayment | Number | | Y | |

| | | | | | |
|---|---|---|---|---|---|
| 58 | Date of last repayment | Date | | Y | |
| 59 | Date of filing of suit | Date | Date of filing of suit by the Creditor against the Debtor | N | Required for Operational creditors if available.<br>Not required for banks |
| 60 | Supporting documents | Attachment | Attach documents such as repayment schedule, account statement, any supporting documents for proving default | Y | |