NeSL
National E-Governance Services Ltd.

Information Security framework

The emergence of new technologies and tools is increasing organization's exposure to critical vulnerabilities thereby increasing the risk to the organization.
The impact of such incidents may result in serious financial loss along with substantial brand value deterioration

CONFIDENTIAL TO RECIPIENT

National E-Governance Services Limited
Gresham Assurance House, 4th Floor, Sir P.M. Road, Fort, Mumbai- 400001
Email – techsupport@nesl.co.in

Information Security Framework at NeSL

Classic information security approaches are not capable enough to handle the new global rise in cyber security incidents, which necessitates a separate security framework for organizations in the financial sector. With this background, by considering increased exposure to cyber-attacks and incidents, Reserve Bank of India has provided guidelines for cyber security framework which highlighted the need for strengthening the security posture thereby ensuring the cyber security preparedness on a continuous basis. The guidelines are designed to enable banks and other financial organizations in adopting and formalizing a cyber-security policy resulting in proactive threat identification and mitigation.

NeSL Information Security Policy

NeSL has experienced consultants who have assisted in formulating the Information Security Policy. The policy has been framed to facilitate NeSL to progressively adopt a Security framework compliant with ISO 27001:2013 requirements and also adhere to the RBI guidelines on Cyber security framework.

IU Application Security

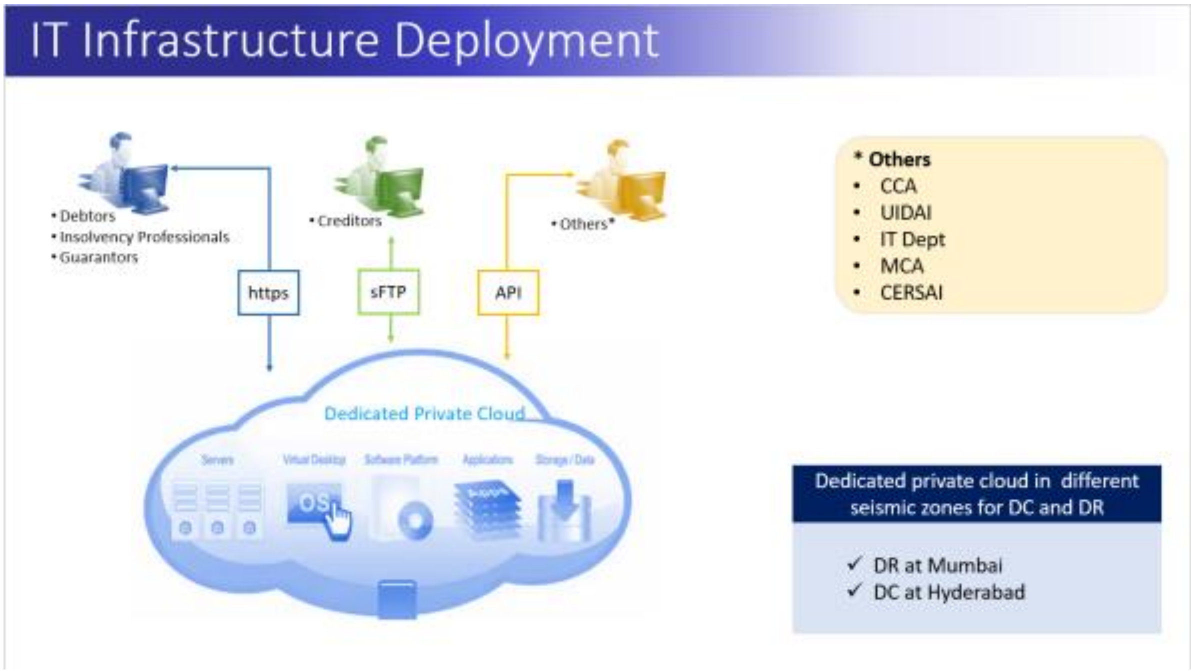
Data Security & Privacy is ensured in the NeSL Information Utility (IU) application as follows:

- Proper audit log is maintained
- Data encryption at transit and rest
- *SFTP*/API calls only from whitelisted IP address(es)
- NeSL's IU platform accepts only digitally signed data. The digital signature public key must be uploaded at the time of registration, which will be used for validation during data submission. This ensures non-repudiation.
- OWASP Standards & IU Technical Standards are being followed
- Only the user who submitted data and the related party to the debt can view data

At the application level the following controls ensure security:

- CSRF access is handled
- HTTPS implementation
- Session management
- Role based URL security, deny access if invalid URL is accessed

A schematic view of the IT Infrastructure deployment and Security Architecture is depicted below:



IT Infrastructure Deployment

- Debtors
- Insolvency Professionals
- Guarantors

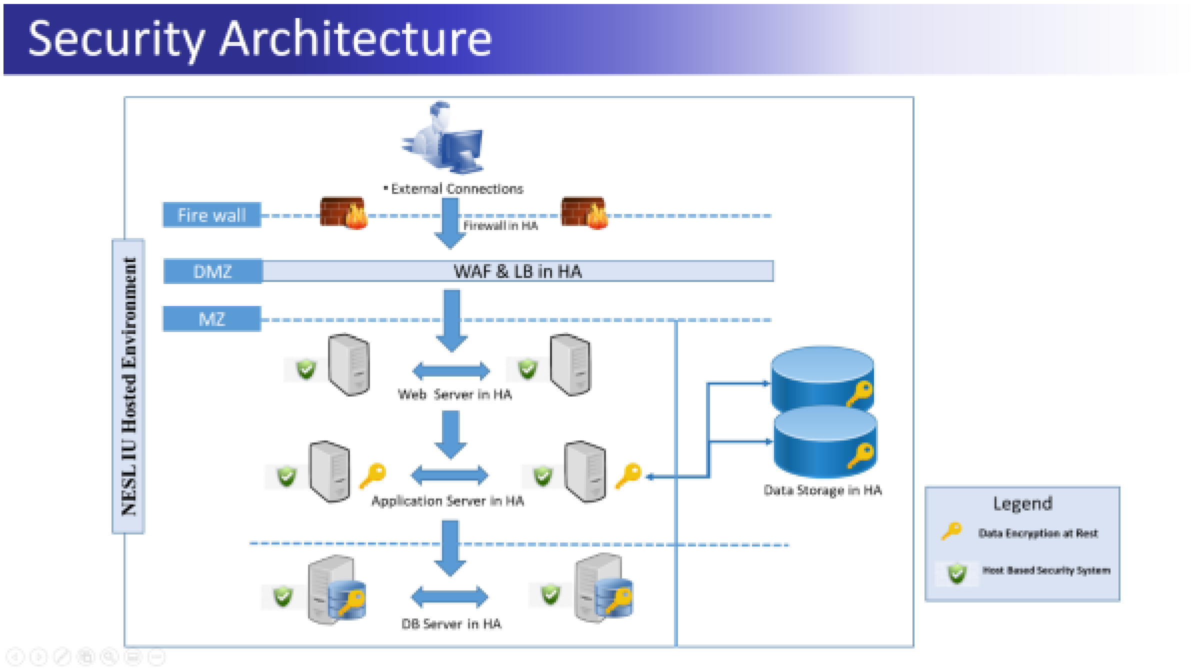
- Creditors

- Others*

*** Others**
- CCA
- UIDAI
- IT Dept
- MCA
- CERSAI

Dedicated private cloud in different seismic zones for DC and DR

✓ DR at Mumbai
✓ DC at Hyderabad



Security Architecture

Legend
- 🔑 Data Encryption at Rest
- ✓ Host Based Security System

Datacenter Security

The IU application is hosted in a Tier 4 Datacenter with the Primary and Disaster Recovery Centers located in different seismic zones. IT Business Continuity plan provides for an RTO of 1 Business Day and RPO of 15 Minutes as per IBBI Technical Standards.

Security Features:

- Host based Security System for the production systems
- Access to the Servers over VPN
- Next Generation Firewall
- Security Information and Event Management (SIEM)
- Web Application Firewall (WAF)
- Managed Advanced Persistent Threat (APT) Service
- Distributed Denial of Service (DDoS) protection
- Physical Security and Safety
- Earthquake resistant civil infrastructure
- CISF designed physical Security
- CCTV Surveillance
- Biometric Access in Data center area

IT Audits

Information Technology (IT) audits can help organizations identify critical gaps in data security and reduce the threat of security compromises. Accordingly, NESL has engaged external auditors to conduct periodic audits as follows:

- NeSL engages CERT-In empaneled auditor to periodically conduct “Vulnerability Assessment and Penetration Testing” of the IU Software to identify and mitigate software security risks and vulnerabilities. As per UIDAI mandate, during every eSign related code change, VAPT is being conducted.
- Similarly, NeSL office IT infrastructure is also audited by CERT-In empaneled auditor.
- Deloitte Consulting was engaged to perform process audit for NeSL’s Information Utility. The audit covered the Information Technology General Controls for IU Application and NeSL IT Infrastructure as follows

    1. User Access Management process
    2. Audit Logging Process
    3. Change Management Process
    4. Backup/Restoration of Data
    5. Patch Management Process
    6. Database, Operating System configuration parameters
    7. Internal office IT infrastructure
    8. SOC management

NeSL conducts audits at regular intervals - VAPT audits of IU Software, yearly audit of Office IT Infrastructure, yearly audit of the Data Centre and Source Code. As per UIDAI mandate eSign code is audited as and when the version changes.

Inspection by Regulator

Our regulator IBBI conducts annual inspection covering all aspects of IU platform.

Technology Committee

NeSL is being advised on technology matters including security aspects, by a technology committee, comprising eminent persons in the field of Information Technology.

NeSL
National E-Governance Services Ltd.

Email: techsupport@nesl.co.in
Toll Free Number: 1800 266 2346