Information Technology Policy And Procedure Manual

Approval Date:-01/04/2023

Review Date- 01/04/2024
Approved By- Abhishek Jain (Director), Abhas Jain Director

Contents

1. Document Review and Approvals

Document Ownership

This document is owned by Nirman Share Brokers Pvt Ltd. – IT Department.

This Document has been reviewed by

Reviewer's Name	Date of
Mr. Tushar Suryavanshi	01/04/2024

This Document has been approved by

Approver's Name	Date Approved
Mr. Abhas Jain	05/04/2024
Mr. Abhishek Jain	05/04/2024

2. Introduction

Nirman Share Brokers Pvt Ltd. NSBL Information Technology (IT) infrastructure has attained unprecedented importance to support the growth. Considering the high dependence on IT, NSBL has also undertaken expansion and up gradation of its IT infrastructure and application landscape.

NSBL has realized the importance of documenting its IT policies and processes to ensure that they are unambiguous, transparent and applied uniformly across the organization. This IT Policy document is the key building block of this initiative.

3. Nature and purpose of the IT Policy document

A policy is a high level statement of Management intent. The key features of this IT Policy are discussed below:

- **Broad guidance**
  The IT Policy will lay down broad guidelines to govern IT processes within the IT Department (ITD). The Management mandates that all processes within ITD will be in conformance to these policies.
- **Long term**
  It is envisaged that these policies will govern the functioning of ITD without significant changes to its composition over a three to five year period.
- **Wide dissemination**
  The IT Policy will be widely distributed and available across the organization. All employees of the company and members of ITD should be aware of the various provisions of the IT Policy and adhere to the same.
- **Strict adherence**
  All employees and members of ITD should strictly adhere to the provisions of the IT Policy. Any violation or wilful non-compliance to its terms may invite disciplinary action by the Company.

4. Applicability of the Policy

The IT Policy is designed by the Information Technology Department and approved by the senior management, and as such, will apply to:

- All employees of NSBL Industries Ltd and its subsidiaries, sales offices, affiliates and users of IT facilities within NSBL.
- All contractors / service providers of NSBL making use of IT facilities
- All employees of the contractors of ITD, to the extent that they are involved in carrying out day-to-day activities for the Company.
- All systems used by ITD (i.e. computer systems, networks, ancillary equipment, storage media etc.).
- Any other area defined by the CIO in a formal amendment to the IT Policy.

5. Document Structure and Control

All documentation associated with the IT Policy is subject to a set of document control procedures outlined in the following paragraphs. These document control procedures play the most important role in that they ensure:

- A high level of quality and standardization is achieved.
- Policy documents and the changes thereof are used only after they have been approved.
- Maintenance and enhancement to the IT Policy is simplified after it has been approved.

6. Document Storage & Control

IT Policies will be made available on the Internal Hosting platform in a secure manner. A considerable amount of associated documentation may need to be recorded. A single master copy of the approved IT Policies should be maintained. The procedures for change management and versioning outlined in subsequent sections should be implemented.

7. Change Control

Any change required in the IT Policies will be documented and forwarded to the CIO through the concerned Department Head.

The CIO will review the request with the help of concerned personnel and will approve/ reject the change suggested in consultation with the top management.

In case, the change request is approved, it will be forwarded along with the changed text to the concerned personnel having access to the master copy for making necessary changes. The latest version will be reviewed, approved and distributed to authorized personnel.

8. Dispensation

IT policies are mandatory in nature and any deviation will require formal approval of the Top Management. The CIO will review the request and will accept/ reject based on the validity/applicability in consultation with approving authority.

The request can be approved for a specific time limit after which it becomes again mandatory to comply with the IT Policies or to apply for extension.

9. IT Organization

IT Steering Committee

- Information Technology Steering Committee (ITSC) will be at the apex level of IT Organization.
- ITSC responsibilities will be adequately documented and conveyed to the members.

- ITSC will meet periodically to assess, review and monitor critical aspects pertaining to IT
- function of NSBL.
- ITSC will set up project committees with relevant positions to monitor and implement major IT projects having critical business impact.

IT Steering Committee Composition

- MD
- Executive Directors
- CIO

Responsibilities of the IT Steering Committee

- ✓ Approving IT strategy, IT budget and IT resources.
- ✓ Approving major IT initiatives.
- ✓ Approving major initiatives to enhance information security.
- ✓ Monitoring progress of major IT initiatives.
- ✓ Reviewing and approving IT policies and procedures, authorization and IT security related policies and procedures.

IT Department

- Chief Information Officer (CIO) will head the IT Department.
- Functional & business leaders and their team would support CIO in formulation and adherence of the IT policy
- Detailed and up-to-date documentation will be maintained giving details of IT Department's organization structure.
- Job responsibilities for all IT functions are defined in such a manner that positions may have overlapping roles but none conflicting, roles & responsibilities.
- Job responsibility for each position will be clearly documented along with the authorization level entrusted.
- IT personnel will possess adequate skill sets to undertake their job responsibilities and to eliminate dependency on specific individuals.

Responsibilities of the CIO

- Lead the IT team of NSBL
- Manage day-to-day IT operations at NSBL.
- Formulate and enforce IT strategy, policy and procedures.
- Approve IT Service requests / change requests.
- Provide relevant inputs to the ITSC to enable the committee to take decisions.
- Assume overall ownership and management of the IT projects.
- Control and monitor the outsourced services.
- Ascertain security requirements as and when required.
- Recruit need-based skilled manpower.
- Ensure continuity of IT services.

10. IT Strategy and Planning

- IT strategy would be aligned to and integrated with the business strategy.
- ITD would prepare the IT Roadmap for NSBL and formulate the IT strategy in the long and the short terms for implementation.
- IT strategy would be developed with the business goal of striking an optimum balance of information technology opportunities and business requirements as well as ensuring its accomplishment.
- CIO would create necessary plans including technology acquisition, staff training and recruitment,

resource allocation etc. to support and implement the IT strategy.

- ITSC will meet periodically to review IT strategy in light of business strategy changes and implementation status of IT initiatives.
- The CIO will ensure that necessary documentation is maintained for:
  - Information architecture.
  - Networks and infrastructure.
  - Engineering / business applications.
  - LAN/PC Support.

11. IT Cost Management

- IT budgets are prepared and approved to maintain current & future IT Infrastructure operations and IT initiatives finalized in the IT strategy as well as the business growth.
- Current operating costs are appropriately analyzed and used as a base for preparing budget and variance analysis.
- IT related costs are tracked, and budget variances analyzed on a regular basis.
- IT related costs will be distributed/recharged to respective departments / cost centers in line with the organizational process as far as realistic and feasible to spread the culture of cost management and ownership.

12. Management Reporting of IT Performance

- Reports are generated on a periodic basis, providing key performance indicators regarding the operation, strategy, projects, security, IT investment, IT personnel etc. and presented to the Management.
- Management reports should be tailored to meet the needs of the business.
- Reports of service levels delivered by outsourced vendors will be obtained on a periodic basis and summary reports will be presented to the Management.
- Feedback regarding IT services will be obtained from users on periodic basis on the user satisfaction levels and summary report will be presented to the Management.

13. Service Level Management

- Service Level Managers will be identified to implement and maintain the Service Level Management process.
- Service level targets and workload characteristics for each service will be agreed with respective users (to the extent feasible) and vendors/service providers and documented in one or more Service Level Agreements (SLAs).
- All SLAs will be subject to change control and be reviewed at least once a year.
- Service performance against the SLAs will be monitored and analyzed at regular intervals. The reports will be made available in a summarized form to the Management.

14. Legal and Regulatory Compliance

- All relevant legal, statutory, regulatory and contractual requirements applicable to each information system are discussed/reviewed with the compliance officer / Company Secretary, explicitly defined and documented on a continuous basis.
- Necessary facility to meet the identified requirements with individual responsibilities for support are defined, documented and communicated to respective individuals.
- Concerned departments will be responsible to report any breach or suspected breach of compliance requirements to its superiors or ITD at the earliest.
- Concerned superiors will initiate necessary escalations to the ITD for subsequent actions on the breaches reported.

15. IT Asset Management

Asset Classes

- Based on the Confidentiality, Integrity and Availability requirements, different types of IT assets merit different levels of protection. Recognizing this, the ITD will categorize its IT assets under different classes and take appropriate measures to protect them.
- All assets will be classified into the following types:
  - Hardware assets (e.g. Server, Desktops, Network, UPS, other Equipment and media).
  - Software assets (e.g. operating systems, applications, Office Automation software, developments tools, and utilities).
  - Information assets (e.g. databases, manuals etc.).
- All IT assets will also be assigned a criticality rating by the owners in consultation with the CIO.
  - Critical (Absence of asset will result in disruption of business; no easy substitute available)
  - Essential (Essential for continuing business; substitutes available)
  - Important (Multiple/ easy substitutes available)

Inventory

- ITD will maintain an inventory of all the IT assets under its purview. The IT asset owners will be responsible for maintaining an updated status of the inventory.
- The branches will also maintain an inventory of IT assets owned by their staff.
- A detailed inventory is maintained by ITD for all hardware/software assets and the software licenses.
- The original media in which the software was acquired, and its license documents will be inventoried and stored in a secure manner.

Labelling

- All physical IT assets will be appropriately labeled to indicate their class.
- The labels will indicate the IT assets' classification and serial number.

Asset Movement

All asset movement - intra-office and inter-office (hardware, media etc.) will be approved and documented.

Insurance

All IT hardware assets will be adequately insured through Electronic Equipment Insurance.

IT Procurement

- All hardware/software assets will be procured in accordance with the standard procurement processes and budgeting guidelines of the Company.
- The Company will select a panel of vendors for consumables at the start of the financial year to expedite the procurement process and review the rates on a periodic basis.
- The procurement and installations of hardware/software assets will be planned in advance and communicated to the concerned personnel/department to ensure minimum disruption to the business operations.

Maintenance and Upgrades

Only authorized patches / upgrades received from the respective vendors will be used for the hardware/software assets. All patches/upgrades will be tested before installation to the extent possible/desirable.

Information Assets

Information assets include data and other elements of information and knowledge base that enhance productivity and security, provide potential competitive advantage or are proprietary to the Company. Examples of such information assets include:

- Database of customers.
- Business/Financial data
- Employee data
- Firewall rule base.
- Router access control lists and configuration files etc.

All officers and administrators of ITD will identify information assets under their custody and initiate appropriate steps to protect them.

Confidentiality Classification of Information Assets

Information assets will be classified into the following categories and marked as such based on their confidentiality requirements and their importance to the Company:

- Public information.
  General release information is widely disseminated amongst the public at large and requires the lowest level of security protection. However, reasonable care may need to be taken to maintain its integrity and correctness.

- Restricted
  Restricted information is made available only to authorized persons, both within and outside the Company (e.g. key service provider, auditors, Banks, regulator etc.).
  Unauthorized access/disclosure of this type of information has the potential to cause financial and/or other collateral damage to the Company or any related party. Adequate security measures will be provided to prevent unauthorized access.

- Confidential
  Information is classified as strictly confidential only if its disclosure would cause serious damage to the Company or any other party to whom the information pertains. Strict security and control measures will be adopted to prevent unauthorized access to this type of information. Confidential information requires the highest level of protection and should be made available only to few authorized personnel of the Company.

Protection of Intellectual Property

- ITD would undertake necessary measures to protect the intellectual property of the Company as well as those of vendors and associates.
- ITD would only deploy and use duly licensed software.
- The Company would assume ownership of all intellectual property (e.g. software, application etc.) developed by outsourced vendors and/or users of information systems during their engagement with / employment in the Company.

Replacement period of Computers and Disposal of Assets

- Replacement period of computers would be 4 years based on the performance after possible up gradation of the computer system.
- All unwanted and obsolete IT assets will be disposed off after clearance from finance and approved by the ITSC in compliance to E-Waste policy.
- ITD will ensure that the assets under its custody are disposed of securely:
  - All data stored on magnetic media is destroyed by low level formatting / degaussing the drives, tapes, disks etc.
  - All printed material containing sensitive data will be shredded before disposal.

16. Managing Third-party Services

Contractual Arrangements

- The roles and responsibilities of the service provider(s) are clearly defined.
- ITD enters into legally binding contracts with all third-party service providers. Such contracts specifically define:
  - Obligations of the outsourced service provider to ensure security and controls for the Company's IT assets.
  - Service levels required from the outsourced service provider.
- ITD defines the objective of outsourcing exercise and will conduct a formal risk assessment before such access is granted.
- ITD requires third-party service provider to seek prior authorization to sub-contract any or all of their responsibilities.

Monitoring

- ITD assigns the responsibility for monitoring the performance of the outsourced service provider.
- The assigned personnel would monitor the outsourced service provider for compliance with the applicable policies and procedures.
- Summary reports are prepared and presented to the ITSC on a periodic basis.

Access Restrictions

- Third-party accesses to IT assets are allowed only in cases where there is a clearly defined business need.
- Third-party accesses to IT assets are granted only on a prior approval of respective asset owner(s).
- Third-party access is provided based on a formally executed contract as far as possible.
- This contract would stipulate that all employees or agents of the third-party are required to comply with all appropriate IT policies of NSBL and will confirm existence and operating effectiveness of all key security controls for the access.
- All third-party vendors have to agree in writing to maintain strict confidentiality concerning NSBL's information.
- The third-party will ensure that all its employees and agents who have access to NSBL's information are aware of and carry out their security responsibilities with respect to the information asset that is accessible to them.
- Accesses to third-party will be granted based on the principle of 'least privilege' and will be based upon 'need-to-know' and 'need-to-do'.
- Accesses to third-party are granted for a pre-defined period of time.
- Third-party access usage would be logged and reviewed on a regular basis.
- Third-party access to NSBL's IT assets and in particular, access to customer data must be in accordance with relevant legal and regulatory requirements.
- ITD reviews third-party access rights at regular intervals for their appropriateness.
- Access rights granted to third-party are removed immediately after the expiry date unless and until it is renewed as per relevant procedures.

17. Operations Management

IT Operations

- The responsibilities for managing and operating computers and network facilities are clearly defined.
- ITD would formally assign responsibilities for managing the operations of individual server room and other infrastructure facilities at the Head Office and other locations (if any).
- All employees responsible for computer operations are formally informed of their duties and

responsibilities when it is assigned to them. They will also be trained on the information security requirements of the operational activities conducted by them.

- All designated employees would follow the procedures and guidelines laid down in key areas of operations to ensure that a uniform, controlled process is adhered to.
- ITD would formally assign administrators such as SAP Basis / Database Administrator, System Administrator, and Network Administrator etc. for the various information systems and related functions under its management. Administrators take up their responsibilities only after a formal assignment of authority.

Helpdesk & Facility Management

- The IT Helpdesk is the central point for reporting and resolving all user queries, incidents and service calls for IT support.
- The Helpdesk is responsible for:
  Recording & addressable of queries and complaints of users.
  Receiving information on viruses and other threats to information systems.
  Escalating all unresolved queries to specialists and vendors
  Reporting query resolution back to users.
  Periodic reporting to the Management.
- ITD appoints dedicated and technically competent resources for Facility Management and Helpdesk Operations region specific.
- A senior and responsible resource is assigned to oversee Facility Management and operations of Helpdesk.

Configuration Management

- ITD would ensure that all system configurations are recorded, maintained and regularly reviewed.
- Procedures are implemented for protection against unauthorized or illegal software and hardware installation.
- Procedures are implemented to classify, approve, release and implement changes.

Planned Disruptions

- Planned disruptions are scheduled, as far as practical, preferably non business hours to ensure minimum impact on system availability.
- Concerned personnel / users are intimated about non-availability of IT service(s) along with the estimated duration with appropriate notice well in advance.

Data Archival

- Past data is archived on a periodic basis based on the system performance, capacity and user requirements.
- ITD will formulate data archival procedures to ensure optimum performance of the IT systems.
- ITD will formulate storage of user email archives.
- Adequate precautions are taken during data archival process to ensure data integrity.
- User inputs will be taken to ensure compliance with business, regulatory and legal requirements for archived data.
- Archived data is stored securely on cloud or external media is managed, tested as per backup policy.

18. Development Methodology

- ITD enters into a formal contract for development and implementation projects being executed by external service providers.
- All outsourced initiatives have Project Managers both from NSBL and the vendor's end formally nominated to manage the process and would be responsible for ensuring the progress in a controlled

manner.

- All outsourced developments would have a "software escrow" clause built in that would enable NSBL to take control of the source codes in case the developer terminates its business or is rendered insolvent.
- The outsourced development projects would also follow the policies defined in this section and exceptions, if any, will be approved by the CIO.

Software Retirement/ De-commissioning

- ITD makes a periodic assessment of the software currently in use in the Company. Based on this assessment, it may decide to retire / de-commission specific software from its inventory.
- In this decision, it may guided by factors like
  - Obsolescence.
  - Vendor support.
  - Cost of maintenance.
  - Lack of effective security and control features.
  - Demand of the software on the existing storage, memory and network resources.
  - Availability of a better alternative.
  - Change in technology
- ITD would formally record its decision to retire / de-commission software. Based on this decision, responsibility would be assigned to specific officers to ensure that the software has been deleted / uninstalled from all relevant servers and personal computers.
- ITD would also ensure the confidentiality and integrity of all data stored in / generated by the software. The data will be made available for future use.
- All retired / de-commissioned software would be archived for emergency use.

19. Change Management

Applicability

- Change management procedure will apply to all changes for all systems including:
  - SAP Changes
  - Business Application changes
  - Database changes
  - Operating System changes, upgrades, patches and service pack installations etc
  - Network changes
  - Platform/Landscape changes

- All change requests would be received in specified written format from users.
- Change requests would be categorized based on business requirements.
- The Projects Head would do impact assessment with inputs from the users and development team, and change requests will be prioritized based on the assessment.
- The impact assessment will consider both business and IT issues.
- All changes to programs and software would be authorized by the Projects Head and User Department Heads.

Testing

All changes are tested before these are transferred to the production environment.

Emergency changes

ITD staff may not have the time to go through the formal process while reacting to emergency situations.

However, in such cases oral authorization would be necessary for executing emergency changes. The

formal authorization process should be availed post-facto at the earliest possible opportunity.

Change tracking

The Projects Head will be responsible for ensuring that all changes requested by the users have been executed to their satisfaction. So a Change Request Form is initiated and is available.
User should be completely involved in the change process. Sign-off should be obtained from the user after execution of changes.

20. Logical Access Controls

User Management

- No person would access any application, information services or data unless and until specifically authorized to do so.
- Each user ID is unique to one user or process, at least, in context of a specific information system.
- No user ID should be shared and users would be responsible for all activities performed using the user IDs associated with them.

- Group accounts or group log-ins should be avoided as far as possible. When there is no practical alternative, a group account may be used with prior approval of Head of Department and CIO, and clear accountability assigned to one individual/group head along with group member information record.
- Default or vendor supplied IDs will be secured as per vendor guidelines.
- Privileged accounts will be strictly controlled and kept to an absolute minimum.

Segregation of Duties

- Access control matrix defining access rights for IT user profiles will be maintained for all IT assets.
- Access rights are defined based on 'need-to-know', 'need-to-do', 'segregation of duties' and 'individual accountability' principles.
- Maker-Checker concept is implemented for the application along with authorization power based on roles / designations and monetary limits.
- Access rights would be assigned to users based on prior approval from the concerned information asset owner.
- ITD would review access rights at regular intervals to ensure that they are justified by current business requirements.

Password Controls

- Passwords of Domain (login Password of Computer), would be of minimum of six (6) characters long with at least one non-alphabetic character, special character and number.
- Passwords would not be shared, written down or stored in an open form, where they may be easily compromised.
- Passwords would not be stored or transmitted in a readable form (i.e. plain text form) as far as possible.
- Passwords would not be hard coded into software as far as practical and possible.
- Initial passwords given to users shall be changed immediately by the user himself.
- Initial passwords would be communicated to the users in a secure manner.
- System generated or initial passwords should be changed by users on first log-in attempt.
- Vendor supplied passwords should be changed before the product is put into use.
- Passwords for critical accounts like privileged accounts should be changed at least every thirty (30) days. User passwords should be changed at frequent intervals.
- Additionally, passwords should also be changed promptly if suspected to be compromised or have been disclosed for a cause.

21. Physical Access Controls

- ITD will designate certain areas of its infrastructure as “Secure Areas”. This will include areas like Data Centre / Server Room / Communication Room.
- Secure areas would be protected by appropriate entry controls like locks, swipe cards, proximity cards etc. to ensure that only authorized personnel are allowed access.
- Access to the secure areas would be limited to authorize users only.
- Access permissions to the secure areas would be granted based on ‘need-to-do’ principle.
- Any article that can cause threat to security and confidentiality of the secure areas and/or the IT equipment installed therein would not be allowed inside the area.
- Appropriate security notices would be displayed inside and outside of the secure areas. Notices will also be displayed prominently inside and outside the secure areas prohibiting eating, drinking and smoking inside the secure area.
- Visitors and temporary staff would be granted access to the secure area strictly on valid business purposes (e.g. maintenance, cleaning, audit etc.).

- All visitors would be accompanied by an authorized IT person at all times during their stay inside the secure area.
- ITD would periodically review the list of users who have access to the secure areas and ensure that such access is granted to bona-fide individuals only.

22. Computer Operations

Infrastructure Set-up

ITD inputs would be taken by the Administration Department before setting up new offices / renovation of old offices regarding Server Room set-up and layout, LAN cabling, UPS cabling, electrical supply, air-conditioning and humidity controls, physical access controls etc.

Standard Configurations

- ITD would decide the standard configurations for Servers, desktop computers, Network equipment, and peripheral devices like printers, scanners etc. and Internet connectivity for the Company across various offices and locations.
- ITD would decide the provisioning, architecting cloud services (IaaS, PaaS, SaaS)
- All external media storage / Pen drives access would be restricted using DLP on the endpoints**.**
- ITD would check all servers / desktops / laptops periodically for any unauthorized software installed and remove the same immediately.

Environmental Controls

- Suitable temperature and humidity would be maintained in the Server Rooms as per manufacturers’ specifications.
- Temperature and humidity would be monitored regularly.
- Dual air-conditioners would be provided in the Server Rooms to ensure redundancy.
- Suitable power supply would be provided to IT equipment as per the manufacturers’ specifications. Especially in power deficient areas, due care will be taken to arrange for additional power supply using UPS / generator sets.
- Critical IT equipment would be protected against power failures and other electrical disturbances with the help of UPS, stabilizers, surge protectors, generator sets etc.
- Adequate fire detection and suppression equipment like smoke detectors, fire extinguishers would be deployed in Server Rooms and other office areas.

Logs and Audit Trails

- The owners of information systems would be responsible for defining the requirements for logging specific events and transactions.
- ITD would ensure that defined events are logged. The logs would be reviewed at periodic intervals.
- Logs and audit trails will be maintained for all:
  - Applications
  - Operating Systems
  - Database
  - Firewall
  - Internet access (as & when required)
  - E-mail (as & when required)
- Access to logs would be strictly controlled.
- ITD would assign responsibilities for monitoring such logs.
- All exceptions would be escalated to the asset owner.

23. Network Security

- Network security architecture is defined, documented and implemented.
- All external and third-party connections are adequately secured.
- Platform specific security standards including hardening documents for network components are maintained and implemented.
- Network security architecture is reviewed and updated on a periodic basis.
- Any change to the network security architecture would require prior approval of CIO.
- Appropriate security logs will be enabled on all networks and reviewed on a periodic basis.
- ITD will ensure that the data cable terminations at all office locations are documented and maintained. These will clearly indicate the logical connections and physical locations of the equipment on the network. (E.g. hosts, hubs, switches, routers, servers, firewalls etc.)
- All changes to the network infrastructure should be immediately reflected in the documentation.

Security Architecture

- ITD would ensure that the network security architecture is well designed and documented.
- ITD would ensure that the security architecture is vetted by external security consultants, if required.
- ITD would ensure that Firewall, Intrusion Detection System and Virus Scanners are implemented at all gateways.

Remote Access

Only selected, authorized users will be given remote access to the Company network.
All remote access to the internal network of NSBL, including E-mail facility will be granted after a dual authentication of the user's credentials.
Remote access to applications / databases can be allowed to a limited extent provided proper secured infrastructure is made available.

Encryption

Appropriate encryption technologies would be employed to ensure security of data and information that are transmitted over network (LAN, WAN and Internet) or are stored in non-secure locations.

Personnel Security

- The job profile of every employee should be designed to include the IT security issues and bind the employees to adhere to the security policy of the Company.
- The Company will ensure that appropriate background and reference checks are carried out before recruitment of employees.
- All third-party service providers such as contractors etc. would also be subject to similar screening. Firms providing contract workers will be required to declare, in writing, that appropriate character and business references have been obtained for the temporary staff deputed at the Company premises.
- The Company would provide its users with adequate training in security procedures and the correct use of information processing facilities.
- The terms and conditions of employment for all employees of the Company would cover adherence to the IT policies.

- All employees and temporary staff are required to sign confidentiality and/or a non- disclosure agreement binding them not to disclose any information, which is classified.
- Non-compliance to IT policies would be dealt with seriously and appropriate disciplinary action taken based upon the nature and extent of non-compliance.
- Necessary controls would be put in place to ensure that employees who leave the Company do not take along with them any resource of the Company, which will hamper its operations and expose it to security risks.
- The Company would introduce a system of ITD sign-off in the joining / transfer / exit procedures. The ITD would have to sign off on the user-id / email-id / access rights creation / deletion etc. before the employee joins / leaves the organization.
- When employees are transferred from one department / location to another, or role changes due to promotion etc. the access rights to network / folders / application should be reviewed and changes made in accordance with new role / department / location immediately.
- Annual check of all user rights would be conducted by ITD with help of asset owners and department heads to ensure redundant user-ids and access rights are rectified.

24. End-user Computing

Data Security

- Users must not share their passwords to the IT /Systems or with any other user.
- Users would be provided necessary training to enable efficient and safe use of computers.
- Specific training on applications usage would also be provided to users. User manuals and 'Help' documentation would also be provided in hard copy or online format as may be feasible and practical.
- Users would also be trained to report any suspicious activity / incidents observed by them.
- End-users may ensure backup of critical data stored on their hard disks on a regular basis. Designated space can be provided on the file server/cloud storage to store data backup.
- End-users are not allowed to download or bring in any unauthorized software, games, etc. from the Internet or from outside and install in the computer provided for their work. Any violation would be subject to management action
- Users are not allowed install any unlicensed software in their machines. Non-adherence would be taken up for management action.
- Users must not share any folders on their hard disks to others as far as possible. All shared folders will be rights enabled. End-users must use designated access controlled space / folders on the file server to share only business documents with others.
- Users must not keep Personal Data files, Photos, Movies in Desktop / Laptop or in file Server.
- A central inventory of end-user hardware, software is maintained.

Clear Desk, Clear Screen Policy

- All information system users are required to follow the "clear desk policy" wherein all confidential Company information should be kept in closed areas of under lock & key when not in use. This includes laptops, correspondence, documents, diskettes, other computer media, manuals, etc. No printouts should be found lying in the printer.
- All computers have to be shut down or the workstation locked under special circumstances when employees are not at the desk or leave the office premises for the day. Alternatively, password protected screensaver will be enabled on all computers with a timeout period.

25. E-mail Policy

To stipulate a policy framework for ensuring all business communication needs of NSBL are met and the utilization of organizational electronic communication resources is optimal. This policy is applicable to all NSBL employees. It covers emails located on NSBL desktops/laptops and servers operating both as standalone systems and from within NSBL networks.

- All users are refrained from using any Email account other than the corporate account for official Email communications.
- Third-party / vendor personnel will be issued special Email IDs which will help them carry out the assigned work and would distinguish them from NSBL employees.
- Necessary controls should be implemented to ensure that employees are not able to send spam Emails. Messages, which are required to be broadcast to all NSBL users or group of users, will be sent by the approved sender.
- Adequate authentication system is implemented for Email to avoid fraudulent use. Any exception will need specific authorization and approvals.
- ITD will define the circumstances under which it would intercept or otherwise monitor the Emails sent through its electronic mail infrastructure.
- All incoming mails will be scanned for virus and other malicious content.
- ITD prohibits transporting specific types of attachments (e.g. .vbs, .js, .exe, etc.) through its Email system on account of potential security risks and unwanted bandwidth usage.
- ITD has fixed a limit on the size of attachments on the Email sent within NSBL and from NSBL to other domains.
- All electronic mails originating from the Company's Email infrastructure to outside domains need to have a formal "Disclaimer Statement" appended to it.
- Employees are advised to use the spell checker before sending out emails.
- Employees should always use standard email signature with his/her name, Job title, company name and other contact details.
- Attachments should be compressed wherever possible.
- If you forward mails, state clearly what action you expect the recipient to do.
- Only mark emails as important/priority if they really are of importance and priority.
- Do not write emails in capitals, that's rude and can upset people in other geographies
- Do not subscribe to a newsletter or news group without prior permission from your supervisor.
- Do not use the electronic mail resources for personal monetary gain or for commercial purposes that are not directly related to NSBL business.
- Do not send copies of documents/software in violation of copyright laws.
- Do not use email systems for any purpose restricted or prohibited by law.
- Do not forward mails to public email service providers (hotmail, yahoo, Gmail etc.).
- Do not indulge in "spoofing" (i.e., constructing an e-mail communication such that it appears to be from someone else instead of you).
- Do not attempt unauthorized access to email or breaching the security measures on any electronic mail system.

- Do not send mail addressed to all employees without consulting IT and your HoD
- Do not make or post indecent remarks, proposals or materials through email
- Do not forward MP3, irrelevant JPEGs or other image files through email
- Do not send mass greeting cards.
- Do not forward email to multiple addresses unless it serves genuine business purposes.

26. Virus and Malicious Code Security Policy

ITD ensures that a comprehensive virus protection program is instituted across the organization.
ITD ensures that the latest anti-virus protection is available on all identified systems (e.g. file servers, mail servers, desktops, laptops etc).
The virus definition files are updated with the latest patches as soon as the vendor makes them available.
All virus alerts are expeditiously responded to and attended to as per the incident reporting and management process.

27. Business Continuity / Disaster Recovery Planning

Backup of Data

ITD would lay down processes to ensure that all information assets of the Company are backed up periodically and stored securely for retrieval when necessary.
The asset owners are responsible for defining the backup requirements of the information contained therein. This is based on the availability requirements of the application and the information contained therein. Examples of assets that will be considered are:

- Application databases
- System data (e.g. system files, application configuration files, source codes etc.)
- Development data (e.g. source codes, test database, test results etc)
- Firewall rulebase
- Router configuration files and Access Control Lists ("ACLs")

The backup requirements would define the following:

Backup frequency (i.e. online, daily, weekly etc.),
Nature of backup (i.e. full backup, incremental backup),
Recovery Time Objective ("RTO", i.e. the time period within which the information needs to be restored in the event of non-availability of the primary data).
The RTO would influence the manner in which the backup media is stored. For example, data with a very low RTO cannot be stored in an off-site location that is situated far away.

The backup requirements would be formally documented and be made available to all backup administrators. Any changes to the backup process will be updated the same day the change has been approved.

Exited user's data Backup

Backup of the exited users data would be backed up on request in a shared external storage device assigned for respective department data backup and handed it over to the requesting department.

Responsibility of Executing Backup Procedures

ITD will assign responsibility to a team/ individuals to execute the backup in line with the agreed backup requirements.

Restoration

All backup media will be periodically tested for restoration.
ITD will delegate responsibility for testing the restorability of the backup media to identified team member(s). He / She will be responsible for :

- Developing a rotation plan for testing the restorability of the media.

- Testing on a periodic basis.
- Confirming the success/failure of the restoration process.

Storage and Movement of Backup Media

- Media will be labeled as per standard labeling convention.
- Media will be stored in a safe and secure environment, in accordance with manufacturers' specifications.
- Media of Operating System and Software, paper Licenses of Software, agreement copy with Service Provider are recommended to be stored in Fire Proof Enclosure / cabinet.
- Only authorized staff members will have access to and control over the media on which the data is stored.
- Media will be physically verified on a periodic basis.
- Media will be removed and/or restored only after appropriate authorization.
- Media will be retired as per manufacturers' specification.
- Media will be disposed of securely and safely when no longer required.
- One copy of the backed up information will be stored at an off-site location. This location will be under the control of the Company and will offer a comparable level of security to the backed up information as at the primary site.
- Movement of media will be controlled to ensure that it is transferred, received and stored appropriately.
- Movement of backup media will be controlled to ensure that:
  - All media scheduled to be transferred on a certain day has been transferred.
  - The transferred media relate to the appropriate backup period (e.g. for a daily tape movement schedule, the tapes actually being transferred do not contain two days' old data).
  - The correct number of backup media is received at the receiving location

Disaster Recovery Plans

- ITD will develop and implement a disaster recovery plan ('DRP') in order to minimize the impact to business activities from failures or disasters, and to continue at an acceptable level of IT operations through a period of unplanned business disruptions.
- ITD will assign responsibility to an individual for managing its DRP initiatives.
- ITD would undertake periodic testing and maintenance of the disaster recovery plan to ensure that it is up-to-date and effective.
- ITD would institute a formal change control mechanism to ensure that implications of any changes to the plan are identified and disseminated prior to up-dation and redistribution of plans.

28. Compliance and Audit

- All persons working in NSBL including third-party / vendor personnel must comply with the IT policies and procedures.
- Independent system audits would be carried out regularly to ensure compliance with IT policy, procedures and security standards across all offices of NSBL.
- The scope and timing of the audits would be planned and agreed in advance with respective auditees.
- Independent pre- and post-implementation audits would be carried out to ensure that the concerned application(s) and/or application change(s) have a sound control environment and they adhere to the relevant IT policies and procedures.
- The access to system audit tools and analyzers would be adequately controlled to prevent possible misuse or compromise.

29. Website Policy

Website Content

All content on the business website is to be accurate, appropriate and current. This will be the responsibility of Corporate Communications department.
All content on the website must follow relevant business requirements such as a business or content plan etc.

The content of the website is to be reviewed every quarter. Basic branding guidelines must be followed on websites to ensure a consistent and cohesive image for the business.