



PROUD TO BE INDIAN
PRIVILEGED TO BE GLOBAL

Information Security policy

LNJ Bhilwara Group

Version 3.8

© LNJ Bhilwara Group

This document contains confidential and proprietary information of LNJ Bhilwara Group Information Systems, the disclosure of which would provide a competitive advantage to others. As a result, no part of this document should be disclosed, used, duplicated, reproduced, stored, copied, transmitted, in whole or in part, in any form of manner or any means- electronic, photocopying without the express consent of LNJ Bhilwara Group management.

This document shall remain the property of LNJ Bhilwara Group's Information Systems and this restriction does not limit the rights of the recipient to use information contained within the document if it is obtained from the approved and authorized source without any restriction.

Ver. No.	Release Date	Description	Author & Owner	Approved By
1.0	August 2010	Initial Release	Company Head for IT	MD
2.0	March 2013	Revised Version	VP(IT)	Management
3.0	December 2014	Revised Version	VP(IT)	Management
3.5	September 2017	Revised Version	GM (IS) & CIO	ED
3.6	April 2019	Revised Version	GM (IS) & CIO	JMD
3.7	August 2021	Revised Version	DGM (IT) & Dy. CIO	JMD
3.8	August 2022	Revised Version	Lead (IS) & CIO	JMD

Modification Details

Ver. No.	Release Date	Details of Changes
2.0	March 2013	<ul style="list-style-type: none"> • Audit Observations & Recommendations • Feedback from IT and Users • Business and Statutory Requirements
3.0	December 2014	<ul style="list-style-type: none"> • Audit Observations & Recommendations • Feedback from Users • Campus/ Colony desk-tops and laptops • Audit Observations of ERP • Wi-Fi Network Usage
3.5	September 2017	<ul style="list-style-type: none"> • Additional Sections with new controls included as per industry best practice. • Obsolete controls removed.
3.6	April 2019	<ul style="list-style-type: none"> • Annual review of the IS policy • Controls reviewed across all the sections for new inclusion and feedback and inputs received from business users, IT Heads.
3.7	August 2021	<ul style="list-style-type: none"> • Annual review of the IS policy • Controls reviewed across all the sections for new inclusion and feedback and inputs received from business users, IT Heads.
3.8	July 2022	<ul style="list-style-type: none"> • Annual review of the IS policy • Suggestions/observations received from Auditor (GSA & Associates LLP) • Controls reviewed across all the sections for new inclusion and feedback and inputs received from business users, IT Heads.

Table of Contents

S. No	Topics	Page No
1	Information Security policy	4-5
2	Scope and Coverage	6-7
3	Policy document update guidelines	7-7
4	IT Asset Life Cycle management Policy	7-10
5	IT Infrastructure Security controls	10-16
6	Data Centre and Network Security	17-23
7	E-Mail Access Policy	23-29
8	Internet Access Policy	29-34
9	Access Control Policy	34-37
10	ERP Application Security Policy	37-38
11	Password Management Policy	39-40
12	Anti-Virus Policy	41-42
13	Software License Management Policy	42-44
14	IT Helpdesk Management	44-45
15	Backup and Restoration Policy	46-49
16	Data classification Policy	50-52
17	Incident management Policy	53-53
18	IT Budget, Training &Skill development	54-55
19	Change Management Policy	55-57
20	Annexure/Forms	58-60

1. Information Security Policy

- 1. Introduction:** The role of Information Technology & Internet as a business enabler has been increasing and becoming vital to success the business. Due to the very nature of this technology, the threat of security of business information and information systems is becoming very critical. It is essential to know which of the organizations resources need protection so that intellectual property of the organization is kept safe and secure. The same is true when exposing organization access on the Internet or even on local area network. With the consumerization of Technology and the employees becoming empowered, ensuring security of information has become critical to survival of business. The information security policy and processes, therefore, are required to be made an integral part of day-to-day business so that we can leverage this technology for business, while at the same time, protect our information and our systems from internal and external threats for business continuity.
- 2. Vision:** To Leverage Information Technology for business transformation while ensuring the safety and security of Information assets and its underlying systems for uninterrupted operation through controls while aligning with the current and future requirements of business.
- 3. Mission:** To protect the information, its infrastructure and applications with build capabilities to prevent and respond to threat, vulnerabilities and minimize damage from incidents.
- 4. Objectives:** The Information Security policy document defines the policies to be followed by all staff of LNJ Bhilwara Group hereinafter referred to as 'LNJB'. The policy

governing Information Technology deployment will guide the development of a well-found information system in order to deliver convenient access to information, improve communication and ensure a flexible and reliable system responsive to the evolving business environment. Controls documented in this policy manual shall enable security over Systems and applications and help manage Information System risks effectively. The key objectives of Information Security policy are: -

- a. To implement information security controls across the LNJB business functions, - for ensuring the Confidentiality, Integrity and Availability (CIA) of information
- b. Create a security assurance framework and strengthen the regulatory, statutory requirements
- c. To deal with threats which are:
 - i. Intentional :(an individual cracker/hacker or a criminal organization)
 - ii. Accidental e.g., computer malfunctioning or an "act of God" such as an earthquake, a fire or a tornado
 - iii. Unintentional, poorly written software applications and scripts, not performing regular security audits, un-patched servers and network devices, inappropriate network architecture, improper segregation, allow attackers to compromise the Cyber/IT security systems or collect data from backend databases.

5. Focuses:

- **Confidentiality:** Only individuals with authorization should access data and information assets.
- **Integrity:** Data should be intact, accurate and complete, and IT systems must be kept operational.
- **Availability:** Users should be able to access information or systems when needed.

2. Scope and Coverage

2.1 This policy applies to following Group companies:

a. Textiles Sector

- i RSWM Ltd.
- ii Maral Overseas Ltd,
- iii BMD Pvt. Ltd.
- iv Bhilwara Technical Textiles Ltd.
- v BSL Ltd.

b. Electro-Graphite

- i HEG Ltd.

c. Power Sector

- i. Bhilwara Energy Ltd.
- ii. Malana Power Company Ltd.
- iii. AD Hydro Power Ltd.

d. Services Sector

- i. ICCS Ltd.

e. LNJ Institute

- i. LNJ Skills,
- ii. LNJ Rozgar.

f. Stakeholders

The Information Security policy applies to all users of LNJ Bhilwara Group and its companies at:

- i. Corporate Office
- ii. Manufacturing Units
- iii. Marketing and Sales Offices

- iv. Extended work-centers at home
- v. The users will include:
 - 1. Employees
 - 2. Temporary staff & Auditors (Statutory/Internal)
 - 3. Consultants
 - 4. Contractual employee

3. Policy Document Update Guidelines

3.1 Document Process guidelines

- a. Information Security policy shall be issued post approval from senior management.
- b. The Information Security policy to be owned by Group CIO.

3.2 Implementation/Enforcement of Information Security controls

- a. IT department in coordination with business shall implement the controls as documented in this policy.
- b. Security Department shall oversee the overall implementation and management of Information security controls to ensure compliance. All Noncompliance shall be reported to CIO for necessary action.

4. IT Asset Life Cycle Management Policy

4.1 IT Assets standard control shall be followed towards demand, planning, procurement, operation, maintenance, replacement and disposal of Assets to ensure compliance at each stage. The IT Assets encompass the following: -

- a. **Hardware:** Servers, Desktops, Laptops, Storage, Printers, scanners etc.
- b. **Software:** Operating Systems, Email System, Business application, monitoring and tracking applications etc.

- c. **Network Equipment/devices:** Switches, Firewalls, Routers, Anti-Spam device Bandwidth optimizer etc.

4.2 Asset Acquisition controls

- a. IT assets procured are to be identified by allocating a Unique Asset ID and are to be recorded through Inventory to ensure these are tracked from purchase till disposal
- b. For each asset, details pertaining to date of purchase, vendor, physical location of the Asset, Annual maintenance Contract (AMC) and Asset disposal/decommissioning time to be recorded.

4.3 Asset allocation and usage controls

- a. The IT Hardware assets i.e. Desktop/Laptop or any other computing/storage device which can store information shall be allocated to Employees, Consultants, auditors or any Third party users based on requirement of job and with approval of Chief Operating officer (COO)/Business Head (BH)/Corporate Function Head (CFH).
- b. The default admin privilege passwords of the system shall be changed by the IT department, prior to issue of asset to user.
- c. Users shall be allocated with one Asset i.e. Desktop or Laptop. However, in case, more than one asset is required by the business user, approval from BH/COO/CFH is required.
- d. Servers, Network devices and other IT assets required as part of Data center shall be fully tested, assessed for fitness of purpose, hardened to security standards and formally accepted by IT department before being deployed to the live environment.

- e. Details of Asset installation for new joiner and Asset movements within the organizations shall be stored/recorded through IMAC (Install Move Add Change) request fulfillment process.
- f. All IT Assets shall be insured through Local Commercial/Administration department in consultation with Location IT department.
- g. In order to ensure traceability and accountability, assets being sent outside the organization (except hard Disk) for repairs/disposal shall be accompanied by a Gate pass duly signed by the local IT department.

4.4 IT Asset Salvage and Disposal controls

- a. IT assets which have reached end of their useful life shall be moved for proper disposal based on management decision and approval.
- b. At the end of asset lifecycle, the same shall be marked as retired/inactive and properly disposed of with all information removed from the system in irreversible manner.
- c. All data are to be deleted, licensed software un-installed configuration setting removed, User Ids, passwords etc. shall be permanently deleted and system to be formatted prior to disposing off the system.
- d. Computer equipments are not to be disposed off via dumps, landfill dustbin etc. Each location will have Electronic recycling bins or space allocated which may be used to store/dispose of electronic equipments.
- e. The salvaged assets can be disposed of through following options: -
 - i. Selling/Donation to employee, NGOs, social organizations
 - ii. Buyback
 - iii. Through e-waste Recyclers.

- f. E-Waste process:
- i. All Group companies which fall under the bulk consumer's category as per statutory requirements, the IT equipment which has been decommissioned and e-waste generated must be channelized to authorized collection center(s) or registered dismantler(s) or recycler(s) or are returned to the pickup or take back services provided by the producers.
 - ii. Record of e-waste (Electronic/IT Waste including all IT Hardware Assets and Consumables) being generated is to be kept in an e-waste Log.
 - iii. All e-consumables including optical mass storage and rewriteable media, including compact disks (CD, CD-RW, CDR, CD-ROM), optical disks (DVD), and magneto-optic (MO) disks, tape, hard drives, flash drives, etc. must be disposed of through e-waste Recyclers.

5. IT Infrastructure Security controls

5.1 Desktops and Laptops

- a. All Desktops and Laptops issued to users shall be configured by IT department with licensed Operating system and applications to execute the job function as per business requirements.
- b. Software or tools which are not required for executing business functions shall be disabled/removed prior issuing the desktop/laptop to the users. If there is justifiable business requirement, the same is to be raised to Service Desk after approval from functional manager/HOD and CIO.
- c. Users shall not be allowed to install any software onto their desktops/laptops.

- d. If an additional software package to be installed to accomplish a legitimate business function, users shall initiate a service request. Post approval from functional manager/HOD & CIO, the IT department shall process the request.
- e. Desktops/ laptops users across organization shall have User profiles authenticated and managed through Active Directory services.
- f. Users requiring any IT service are to raise their request to Service desk for necessary resolution by the IT department.
- g. The Office IT Assets shall be used for official purpose.
- h. Users should properly shut down the system before leaving the office.

5.2 Personal Desktops, Laptops & Other Devices

- a. This Information Security policy controls shall be applicable to all Users, and devices, desktops and laptops or any other communication device while using the Organization's network within the campus/colony or through secured VPN channel.
- b. Users shall declare their personal assets like desktops, laptops, pen drives or any other storage devices at the Security Gate, both at the time of entry and exit.

5.3 Visitors Laptops & Other Network Devices

- a. Visitor access to internal systems and applications for legitimate purpose shall be approved by a Plant IT Head and concurred by CIO.
- b. For visitors (auditors, vendor etc.) to execute certain official task IT department shall provide a PC/Laptop from internal sources provided it's available at the respective location. Visitor's own Laptops or devices, if at all required to be part of the network (after justifiable approval), shall be done so only after applying all LNJB policies through AD.
- c. Visitor's access rights from applications to be deleted immediately post completion of the scheduled task.

- d. Devices/Laptops of the visitor which pose a threat to the organization network shall not be connected to organization network.
- e. Visitors should not be allowed to carry any portable media without permission.

5.4 Printers/Plotters:

- a. All network printers to be configured with IP address and correct host names.
- b. Organization printers should not be exposed to the public Internet.
- c. All unwanted services are to be disabled from the printer.
- d. Printing of software and product manuals, other educational and training materials shall be authorized by functional/department or Location Head.

5.5 Software

- a. All Software applications shall be licensed.
- b. All Licensed Software's and applications shall be tracked and monitored - to ensure compliance towards Software License management.
- c. Use of unlicensed or pirated software shall be strictly prohibited. Any violation to be considered as a serious misconduct and disciplinary action to be invoked against those found guilty. Open source may be allowed based on detailed study and for a specific business purpose.
- d. All Software upgrades and other security patches as required shall be controlled and managed as per the terms and conditions defined by the OEM's and service partners.
- e. The requirement of new software if any is to be duly justified and approved by HOD is to be forwarded for IT for further N/A for acquisition, induction, operation and maintenance.

5.6 CD/DVD and USB Security controls

- a. "Write enabled disc"(CD/DVD) drives shall be removed/disabled from existing users' workstation.

- b. The USB ports of user's desktops and Laptops shall be disabled
- c. Based on legitimate and justifiable business requirement, supported by approval from Business Head/Chief Operating officer (COO)/ CFH only selected users within department shall be granted with USB access for executing legitimate business task.
- d. For corporate users USB ports would be enabled based on legitimate and justifiable business requirement supported by approval from Head of department or CIO.

5.7 Business Application Controls

- a. Applications used for assisting business processes at a particular location shall be termed as Local application and applications managed centrally and being used at all location shall be termed as corporate application.
- b. For implementation/modification/customization/enhancement of any business applications, active involvement of following is mandatory: -
 - i. Respective business function who owns the Application
 - ii. Functional Managers for respective Modules
 - iii. IT Manager who are expected to maintain/manage this application

5.8 Operating system and Application Patch management controls

- a. For all licensed applications and operating systems, the patches shall be acquired from vendors, OEM's as per the terms and conditions defined in the contract/agreement.
- b. All patches are to be tested prior to deployment.
- c. A patch cycle should be in place for facilitating application standard patch releases and updates. The patch cycle shall be configured for automatic or manually update, based on the critical nature of business.

- d. The automatic update flag shall be enabled at desktops and laptops to ensure all the Operating system patches are updated regularly. The patches and updates in the servers are to be updated/installed manually post testing and analyzing the relevance of the patch/update as released by the vendor. Manual patching activity for servers/systems shall be completed after office hours
- e. In case of any anomalous behavior observed post deployment patches, then these patches are to be uninstalled and appropriately investigated by engaging with respective OEM/Vendor before these patches to be installed again.
- f. The relevant patches/updates which are not installed due to system/application dependency or any architecture challenge to be documented as an exception and this to be notified to the CIO.
- g. For highly critical patches, an emergency patch process to be initiated and the patches to be tested and deployed without any delay or wait for scheduled process
- h. Quarterly report to be generated to check and verify the Operating system patch compliance across all systems and notify the patch noncompliance details to respective location IT department for any corrective action.

5.9 Server Security controls

- a. Servers shall be physically located in an access-controlled environment and access to these servers over Local Area Network shall be allowed only to respective administrators.
- b. All server configuration and settings shall be documented and maintained as part of technical guidelines for future reference.
- c. The server shall be installed with licensed Operating system, Antivirus and other business applications as required for executing any business functions.
- d. All Servers shall be updated with correct Service pack as per the guidelines from Original Equipment Manufacturer (OEM).

- e. Any configuration changes for production servers shall follow the appropriate change management procedures.
- f. All Services and applications that are not required shall be disabled and always a standard security principle of least required access to perform a function must be followed.
- g. The most recent security patches shall be installed on servers as soon as possible (after testing the patches); the only exception being when immediate application would interfere with business requirements.
- h. In case the installation of patching requires downtime, the same shall be scheduled appropriately so that it does not interfere with regular working of the users.
- i. All security-related events on critical or sensitive systems shall be logged and audit trails saved as per business and audit requirement.
- j. The audit trail shall be active at all times and separate approval shall be in place for disabling the audit trails should there be any performance issue with respect to Server/systems.

The following information regarding Servers in use shall be maintained Server location

- i. Server Hostname.
- ii. Server type (Physical/virtual)
- iii. Operating System/Version.
- iv. Main usage of the server
- v. IP Address details.
- vi. Server type
- vii. CPU, Memory, Hard disk

5.10 Work from Home Policy:

Work from home is a concept where the employee can do his or her job from home. The purpose of Work from Home Policy is to optimize resources for the company benefits while limiting the security risks.

- a. Define who is eligible to work from home: Not all job functions can be conducted remotely. BH/COO/CIO has to clearly lay out which teams are eligible to work remotely, and which have to be in the office so that hybrid work model is clearly available to all workers to examine.
- b. Establish an approval process: Likewise, once establish eligibility criteria, employee has to take approval from concerned BH/COO & CIO for work from anywhere facility.
- c. Maintain security standards: IT department has to ensure encrypted secured Virtual Private Network (VPN) to protect all system users. Employees should avoid vulnerable public Wi-Fi. Instead, they should use secured hotspots/personal Wifi to connect company VPN network. Employees must keep work data on work computers, not personal ones & should only answer emails on work devices or approved mobile handsets.

5.11 Digital Meetings:

- a. Business meetings should be on Meeting Solutions which are procured & approved by IT Security.
- b. Online meeting recording should be with approval from the meeting requester.

5.12 Encryption Policy

Encryption involves encoding data to keep it inaccessible to or hidden from unauthorized parties. It helps protect data stored at rest and in transit between locations and ensure that sensitive, private, and proprietary data remains private. It can also improve the security of client-server communication. An encryption policy helps organizations define:

- a. The devices and media the organization must encrypt.
- b. When encryption is mandatory.
- c. The minimum standards applicable to the chosen encryption software.

6. Data Centre and Network Security Policy

6.1 Network access controls

- a. All connections to the Local Area Network shall be routed through firewall to ensure there are no unauthorized accesses to network/systems.
- b. The organizations network shall be securely designed and managed to protect threats eliminating from both inside and outside the organization.
- c. A network Segregation shall be in place for external and internal facing IT systems and the network devices shall be monitored for any network outage.
- d. All network devices (e.g., routers, firewall, and switches) default/vendor provided passwords shall be changed by the IT Department.
- e. Access rights to the network shall be allocated based on User's role rather than on a status basis.
- f. The Super user or network administrator rights shall not be granted to users for performing daily routine operational task
- g. Remote access connectivity shall be granted to Users across functions that are authorized for specific business purpose and approved by respective Head of department.
- h. Network device inventory shall be maintained and Network topology diagram documented with sufficient detail to manage and trouble shoot the organizations IT networks.

6.2 Physical Access Controls

- a. The organization core networks and other computer equipment like servers, routers, switches etc. shall be located in a controlled and secure environment.

- b. The room where in all the business critical applications hosted at corporate office shall be termed as Data Centre and at remote location or Plants, these would be termed as Server Room.
- c. Access to the Data Centre or Server room shall be restricted and only authorized IT department staff shall be granted access for executing scheduled and pre-defined task.
- d. The list of persons who are required to work inside the Datacenter/Server room is to be recommended by location IT Head and approved by CIO.
- e. IT department shall periodically review and update the User list that has access to the Data center and Server room. Visitor's access to primary Data Centre must have a legitimate business purpose recommended by local IT and approved by CIO.
- f. The entry and exit details of visitor shall be logged and maintained. The log details shall contain Name of the person, purpose of visit and company name/vendor details, date, and time of entry and exit.
- g. Critical Servers and other network equipment at primary Data Centre shall be housed in an environment that has a monitored temperature, backup power supply and fire suppression systems.
- h. Closed-Circuit TV (CCTV) Surveillance Monitoring may be performed to ensure workforce safety and prevent property loss.
- i. CCTV recordings should be retained for at least 30 days for review and investigation purpose.

6.3 Uninterruptible power supply equipment Security controls

- a. Provisions for uninterruptible power supply (UPS) shall be made to provide uninterrupted power supply to all the IT equipment's/facilities. This shall ensure continuity of operations in case of power outage.

- b. Before installing any IT equipment, the IT department shall ensure that the provision of UPS is in place.
- c. IT assets shall be covered under comprehensive insurance to provide cover to any financial loss that might suffer due to unforeseen happenings
- d. No end user IT asset shall be shifted/removed from its location without prior approval from local IT. However, in case of backend IT assets the shifting to be approved by CIO
- e. Periodic testing, inspection and maintenance of the UPS shall be scheduled and records must be preserved for audit purpose.
- f. Equipment should be correctly maintained to ensure its continued availability and integrity in accordance with the supplier's recommended service intervals and specifications.
- g. Only authorized maintenance personnel should carry out repairs and services.

6.4 Environmental Security Control

- a. The data center should have air conditioning and fire suppressing system.
- b. There should be Fire and smoke detectors and these Fire extinguishers shall be checked for extinguisher pressure as recommended by the OEM. The cylinder last checked date and next check date must be specified on the cylinder.
- c. Toxic and inflammable material should not be permitted in Data Centre's.
- d. The temperature and humidity condition in the Data Centre shall be monitored and controlled periodically.
- e. Periodic inspection, testing and maintenance of the air conditioning and fire suppressing systems shall be scheduled and records must be preserved for audit purpose.

6.5 Cabling Security

- a. Power and Telecommunications cabling - carrying data or supporting information services should be underground or subject to adequate alternative protection.
- b. Network cabling should be protected from unauthorized interception or damage, for example by using conduit or by avoiding routes through public areas
- c. Power cables should be segregated from communication cable to prevent interference.

6.6 Remote access connectivity

- a. Users shall be allowed to connect to organization network from remote location using approved remote access application only.
- b. User Access through remote access software shall approved by the respective functional/department Head.
- c. User-id and passwords for all remote access users shall be provided by the IT department.
- d. Users shall safeguard corporate equipment and information resources and notify their functional manager, and IT department immediately of any security incidents /or breaches.
- e. Remote access user list to be reviewed quarterly and actioned upon based on the response received from respective functional manager or Head of department.

6.7 Wi-Fi access connectivity

- a. Across locations/plants Wi-Fi connectivity shall be provided to laptop users for accessing the organization network.

- b. The IT department is responsible for providing Wi-Fi connectivity at meeting rooms, reception etc., where there is limitation in establishing connectivity through wired network.
- c. All Wi-Fi users shall be connected using secured password.
- d. Across the organization to ensure security and to optimize the network usage bandwidth using Wi-Fi network the users would be categorized under different categories.
 - i. Access through Wi-Fi shall be granted and managed as per below classified categories: Wi-Fi access to Senior Management (Company Directors/Owners etc.): Wi-Fi access to be controlled through MAC address binding and restricted to limited number of users.
 - ii. Wi-Fi access to LNJB Employees: Based on Wi-Fi infrastructure deployed at each location, the Wi-Fi access for employees shall be granted either by integrating with User's active directory User id or through a separate Network SSID and password.
 - iii. Wi-fi access to guests and visitors must be password protected with exposure to only external network only.

6.8 Firewall Security Controls

- a. The Network traffic shall be routed through firewall before entering or leaving the organization network.
- b. All firewalls installed should function as per the rule set defined in the firewall implemented basis organization business requirement
- c. Firewalls deployed should be capable of filtering specific type of network traffic, block any unauthorized traffic and protect the organization from data breach.

- d. Firewall should be configured to store log information for a minimum of seven days, in order to track any unauthorized access attempts and for the purpose of audit and investigation.
- e. The firewall, device must be hardened against penetration and reports shall be configured for periodic monitoring.

6.9 Router Access Control

- a. The router shall be placed in a location where physical access is limited to authorize persons only.
- b. Access control lists shall be configured on routers to restrict access to the internal network, and from internal network to external source.
- c. No user accounts shall be configured on the router.
- d. The Enable Password feature on the router must be kept in a secure encrypted form.
- e. All routers across the organization shall be configured with IP address and a User-id and password for managing the same.
- f. The Network Administrator shall have permission to access or configure router and shall maintain the user name, password in vault as part of privileged id process as documented in section 11.
- g. The routers provided by the external vendors for MPLS shall be managed by vendors The LNJB organization would only use the services of the router and will have access to monitor the performance and bandwidth utilization.
- h. Any configuration change with respect to router must be approved in accordance with organization defined change management practice and should be done as per the business requirement.

- i. Access to router using Telnet to be configured with secure tunnel protecting the entire communication path with password protected. SSH protocol to be used for managing the routers.

7. E-mail Access Policy

7.1 Requirement of E-mail Access.

- a. Email accounts shall be set up for each user determined to have a business need to send and receive company email.
- b. Email accounts shall be created for temporary staff, contractors, consultants or other individuals who are authorized to send and receive mails as required by the respective business function.
- c. Based on management decision critical users with in various business functions shall be granted access to Google mail of Injb domain for accessing the mails with a separate Gmail user-id and password instead of Lotus notes email.
- d. Orientation programs for new recruits should include a session on the e-mail policy.

7.2 E-mail ID format for Permanent and contract/temporary Staff.

- a. A unique e-mail ID shall be assigned to the employee/staff in the organization.
- b. Email addresses shall be constructed in a standard format in order to maintain consistency across the company. The email format shall be applied consistently throughout the organization.
- c. No duplicate e-mail allowed to be created. All staff would have a unique e-mail ID is assigned.e.g. If x.y@Injbhilwara.com already exists; then the new ID with x.y1@Injbhilwara.com will be created.

- d. The e-mail ID of a permanent/contractor employee is created in the format as stated below:

<First name>.<Last name>@<companydomain name>.com
- e. Updation of current mobile numbers under the personal profile of users is mandatory for security reasons. The number would be used only for alerts and information regarding security sent by the IT Department. Updation of personal e-mail id, in addition to the mobile number, should also be mandatory in order to reach the user through an alternate means for sending alerts.

7.3 E-mail ID creation and deletion for users

- a. User shall submit request by providing details of employee id/Contract id, Type of email access duly approved Chief operating officer/ Business Head Operations(BH-O)/ Business Head (BH)/CFH.
- b. Based on approval received IT department shall create E-mail ID and implement required access rights to the user by two working days.
- c. For any new email ID created a default password shall be informed to the user by the IT department
- d. User shall change the password to a new one during first log-in.
- e. Password complexity shall be defined as per the password management policy as documented in section 11.
- f. When a user resign /leave the organization the E-mail deletion request shall be initiated by functional manager/Head of Department (HOD) or the Human resource (HR) department
- g. Based on the E-mail deletion request received, IT department shall disable/delete the E-mail access and provide confirmation. As part of handover process, functional manager/Head of Department (HOD) shall ensure that the data/archive of all the business related communication mails of left employee

is kept in a folder and the same shall be retained by respective functional manager or Head of Department (HOD).

7.4 E-mail Client and E-mail Attachments

- a. Lotus notes Email client shall be configured for Users for sending and receiving mails.
- b. Sending messages to external address other than LNJB domain with attachments, shall be compressed using WinZip to have an optimum use of network bandwidth
- c. Users shall not open attachments that are from an unknown untrusted source or unexpected email attachments which may be malicious in nature.
- d. Users are not to click links within email messages unless he or she is certain of the link's safety. It is often best to copy and paste the link into your web browser or retype the URL as specially-formatted emails can hide a malicious URL.

7.5 E-mail Usage

- a. Users shall use Organization provided email system for all business-related communication.
- b. Users shall not send any business related communication email using their personal email account.

7.6 E-mail Disclaimer, Signature and Password Reset

- a. The following disclaimer will be added to each outgoing email.
 - i. *“This e-mail message is only to be used by intended recipients and all others may kindly delete it and notify the sender. Unless expressly authorized by LNJB, the views expressed and the message itself is that of*

the individual sender and recipients are cautioned to check messages/attachments for any viruses before use. Users acknowledge that messages may contain confidential, proprietary or privileged information and that LNJB neither assures nor guarantees integrity or content of messages."

- b. Users are required to keep E-mail signatures (designation, contact information appended to the bottom of each outgoing email) professional in nature.
- c. The IT department or the delegated E-mail admin team shall perform user password resets when requested by the user post verification of identity.
- d. For any password reset, Users shall raise a ticket through IT Service management tool (or may inform thru Local IT).
- e. Auto-save of password in the LNJB e-mail service should not be permitted due to security reasons.

7.7 Mail Box Size E-mail Backup and Retention

- a. Users shall be provided with email storage on organization servers or network storage devices.
- b. The mailbox size for each use shall be restricted to a suitable size or as per overall storage capacity available for mail server.
- c. For Lotus notes user a maximum of 45 days replica of mails shall be made available as part of server storage.
- d. The E-mail system shall provide warning message as a Pop or through mail alert to the user, when his/her user's mailbox size approaches the specified limit.
- e. The size of each incoming and outgoing e-mails shall be restricted as follows:
 - i. 25 MB for mails received (one mail with attachment)
 - ii. 25 MB for mails to be sent. (one mail with attachment)
- f. Users shall maintain a local archive created in the local machine and move for the mails which are older than 45 days.

- g.** Daily backup of E-mail server shall be undertaken in accordance with “Data backup and restoration policy as documented in section 15 of this document.
- h.** Periodic checks shall be undertaken by IT department or E-mail admin team to restore E-mails which are archived/moved in the removable media to ensure data integrity and availability.

7.8 E-mail Security, Phishing attack and Data leakage prevention controls

- a.** Firewalls and E-mail gateway security device shall be deployed at the organization perimeter to detect and filter for spam/junk/unwanted mails in all incoming and outgoing mails respectively.
- b.** Latest version of Anti-virus software shall be installed at Email server and patches/DAT files to be updated regularly.
- c.** For mobile users to access emails a firewall installed at gateway/perimeter shall ensure secure connection.
- d.** Users shall take precaution while opening emails which are suspicious in nature and shall not send any confidential information to any of external email accounts for the purpose of saving this data in any of the external drive/device etc.
- e.** The organization should explore options of Data loss prevention techniques using DLP tool protect against leakage of confidential data.
- f.** The organization mail server shall be configured to block or remove email attachments infected with virus to prevent from spreading in the network.
- g.** It should be within the right of the IT Department to deactivate or remove any feature of the e-mail service if it is deemed as a threat and can lead to a compromise of the service.
- h.** Any security incident, noticed or identified by a user must immediately be brought to the notice of the IT Department.

7.9 Prohibited actions using Corporate E-mail ID.

- a. Users shall not send emails that may cause disruption at workplace environment in any manner. This includes sending emails that are intentionally inflammatory, use of abusive language or which may include information not conducive to a professional working atmosphere.
- b. Users shall not access another user's email account without the knowledge or permission of that user-
- c. He or she shall not make any fraudulent offers for products or services or conduct non-company-related business, send spam mails, chain mails etc. by using the corporate email Id or corporate network.
- d. Users shall not send mails using corporate E-mail id that may cause embarrassment, reputational damage, disseminate defamatory, discriminatory, sexist, racist, abusive, rude, harassing, annoying, insulting, threatening, obscene or otherwise inappropriate messages.
- e. Users are prohibited from automatically forwarding their e-mails to any Internal/ external address within/outside LNJB group network. In case business requirement, same can be done through IT after BH/COO/CIO approval.
- f. Selected business related emails are allowed to be manually forwarded by a user having LNJB email id to another LNJB internal email id or to any external email id marking a copy to the respective business Head/Functional head and such forwarding must ensure that:
 - i. Adequate business rationale is provided by the user who is required to send these mails and these are agreed and approved by the CIO and respective Business Head/COO
 - ii. These emails do not result in an inappropriate disclosure of LNJB Information

- iii. These are not automatically deleted from the LNJB mail server.
- g. The User is responsible for any data/e-mail that is transmitted using the LNJB system. All e-mails/data sent through the mail server are the sole responsibility of the user owning the account.
- h. Sharing of passwords is prohibited.
- i. The 'reply all' should be used with caution to reduce the risk of sending e-mails to the wrong people.

7.10 Security of E-mails/Release of logs

- a. Notwithstanding anything in the clauses above, the disclosure of logs/e-mails to law enforcement agencies and other organizations by the IT Department would be done as per the Government Laws and other applicable laws.

8. Internet Access Policy

8.1 Internet access provisioning and de-provisioning

- a. Internet access shall be granted based on business need duly approved by Chief operating officer/ Business Head Operations (BH-O)/ Business Head (BH)/equivalent. In Head office, restricted internet to be provided by default.
- b. Internet access to users shall be provisioned by enabling the IP address to access the internet.
- c. Internet access shall be removed when there is no business requirement or when there is disciplinary action been initiated arising from violation of this policy.

8.2 Allowed Usage of Internet

- a. Users shall follow the corporate principles regarding resource usage and exercise good judgment in using the Internet.
- b. Users connecting their desktops, Laptops or mobile phones for accessing Internet and E-mails using organization provided internet facility should be able to connect and access only LNJB group approved sites & E-mails.
- c. Acceptable use of Internet for performing job functions might include:
 - i. Communication between employees and vendors for business purposes.
 - ii. IT technical support downloading software upgrades and patches;
 - iii. Review of possible vendor web sites for product information.
 - iv. Reference regulatory or to gather technical information
- d. No user is allowed to use dial up modem or use any other third party provided internet connection for connecting to the Internet using LNJB group provided devices.

8.3 Internet Security Controls

- a. Access control lists (ACL) (allow/deny access Policy) shall be implemented at firewall to restrict access to sites, services which are not deemed to be relevant to the LNJB Bhilwara group.
- b. Users Internet access shall be routed and validated by the rules defined within the LNJB Bhilwara group firewall.
- c. Each Internet service shall be evaluated for applicable security level like only encryption, only authentication or say encryption and authentication both required must be configured appropriately. (*For instance, "telnet" may need both authentication and encryption whereas "http" may only need authentication.*)

- d. By default, as a practice, both Inbound and Outbound FTP services with Internet shall be disabled. When there is a business requirement to enable FTP service, these shall be supported with clear rationale and approved by CIO and these FTP sessions logging must be authenticated using strong password
- e. All information downloaded. to the organization's computing resources via the Internet shall be screened with updated virus detection software prior to use.

8.4 Managing Domain name and Web Site creation for Business

- a. All Domain name registration and hosting with respect to LNJ Bhilwara group shall be managed and maintained by the IT department in coordination with Business users and Corporate Communication department
- b. A list of Domain names already registered and new Domains names which are required to be registered and blocked for future use by the organization shall be maintained by the IT department.
- c. Any web page or the domain hosting shall follow the organization change management process and IT department shall ensure all registered Domain names are active at all times.
- d. IT Department along with Corporate Communication shall ensure for Domains which are not in Use are formally notified across the organization and follow a de-registration process as per the terms and conditions as provided by the hosting sites.
- e. All individuals and/or business units wishing to establish a WWW home page or site should have a business plan and shall engage with location IT Department for implementation and hosting of web page.
- f. The ownership of development of Webpages and its content updating shall be with Corporate Communications department with necessary support from IT department.

- g. Based on business requirement and the complexity of the Web site, the IT department would review the details and either develops the Web page through the internal development team or hire external vendor and get this developed post approval from the respective business with respect to the financial terms and conditions.
- h. Users are not allowed to host personal sites using the LNJ Bhilwara group Internet facilities.
- i. The respective business may use the internet facility to establish new business channels as part of Business expansion which may include different channels like e-commerce, on-line business engagement with customers etc.

8.5 Internet Prohibited Use

- a. Using LNJ Bhilwara group Internet facilities Users shall not indulge in abusive, unethical or inappropriate activities.
- b. Group internet facility shall not be used to conduct illegal activities like gambling, access or download pornographic/illegal material etc. which are considered as indecent, offensive items on the organization's network.
- c. No user shall enter into contractual agreements via the Internet; e.g. enter into binding contracts on behalf of LNJ Bhilwara group over the Internet.
- d. Users shall not indulge in activities related to personal business enterprise, political activity, engage in any form of intelligence collection, fraudulent activities, or knowingly disseminating false or otherwise defamatory materials
- e. Groups Internet facility shall not be used for downloading/uploading any unauthorized /unlicensed software, applications etc.
- f. Users shall not intentionally interfere with the day to day business operation, attempt to gain illegal access to remote systems, perform any Telnet or Port scan the remote system using the group Internet facility.

- g. Users using LNJB Bhilwara group computers, on discovering that they have connected with a web site that contains potentially offensive material, must immediately disconnect from that site and report the matter to the IT department
- h. Users shall not place organization's business sensitive information or other materials like (software, internal memos, etc.) on any publicly accessible Internet computer which supports anonymous FTP or similar services.
- i. The Organization Internet facility shall not be used to access any gaming sites, trading sites, entertainment, pornographic sites, web proxies, etc.
- j. Access to online personal storage accounts to store official information is prohibited.
- k. IT Department may block content over the Internet which is in contravention of the relevant provisions of the Government Laws and other applicable laws or which may pose a security threat to the network.
- l. IT Department may also block content which, in the opinion of the LNJB group, is inappropriate or may adversely affect the network security and productivity.

8.6 Monitoring and Reviewing of the Internet access

- a. LNJB Group management reserves the right to examine E-mail, personal file directories, web access, and other information stored on company computers, at any time and without notice to ensure compliance with internal policies.
- b. Reports or logs to be made available from the firewall for review and monitor to ensure only organization approved websites as defined under various categories are being accessed.

9. Access Control Policy

9.1 Creation of User ID for Domain login, applications, systems and databases.

- a. The Head of department (HOD) or delegate shall raise new user-id creation request by providing details of new joiner's name, employee id /temp contract id, name of applications with access rights is required for the user.
- b. Post approval IT department shall create User-id and password at operating systems, applications and database, grant the role/access rights requested for and share the details to respective functional Manager/Head of Department.
- c. The IT department shall follow organization defined nomenclature while creating User ID in the Active directory:
 - i. The first three letters will define the office location of the user.
 - ii. Next would be the First letter of the group entity ("RSWM, MARAL" HEG) etc. to which the user is employed with.
 - iii. Last would be the employee id of the user (eg: - A User having employee id R00777 from Head office location (NOIDA) will have an AD id as "NODR00777".
- d. For a single user there shall be only one user ID created in the active directory.
- e. User access to other business applications shall either routed and authenticated through User id and password created on the Active directory or a separate User id shall be created on these applications and access granted to the user based on business requirement duly approved by the functional head/ Head of department.
- f. For contract employees and consultants, an ID expiration date, which coincides with the conclusion of the contracted project, should be entered while creating the user-id

- g. Common or generic User Id shall be created for staffs who work on shifts and to be shared with in the specified group of users authorized by the functional manager/HOD
- h. Use of common/shared user-id shall be restricted within the group of people who would be using this User-id and the password should be managed within the group. Users within this group shall be responsible for safeguard and change of password.
- i. Respective department functional manager shall have list of Common/shared User-id and the names of the users who are using the same.
- j. Initial User id created by IT department that are not used with 30 days after creation shall be disabled.
- k. For modification of access rights in applications/databases the users shall raise modification request by providing details of Username, User id, employee id/temp contract id, name of applications/Database, New role/access details duly approved by the functional manager/HOD & CIO and submit the same.
- l. Post approval IT department shall modify the User role at applications/database as requested for and share the details to respective User/Head of Department (HOD).

9.2 Deletion of User ID from applications and database

- a. Users Head of Department or any delegate shall raise the User-id deletion request and provide details of User-id along with names of applications/systems from where the access for the user are to be deleted.
- b. IT department shall ensure Users Access from all applications/systems are deleted/disabled and allocated IT Assets (i.e. desktops, Laptops, softwares, manuals etc.) are returned by the user before providing sign off in the "No Due" clearance document to the user.

- c. Users functional manager shall inform IT department for retaining any specific data back up if required and provide details of the files/folders and the path/location where in these are to be copied.

9.3 User Access review for applications and systems

- a. As part of quarterly user access review process the Corporate IT department shall generate active user-id report from Active directory system (AD) and share details with respective location IT Heads through mail for review.
- b. IT department to seek support from Users Functional manager/HOD and shall review all user accounts for appropriateness and provide confirmation to corporate IT department through mail within three weeks time from the date of receipt of the mail.
- c. For any changes or deletion of user-id, the functional manager shall engage with IT department and get this completed.
- d. All disabled/locked user-id in applications shall be approved by the respective Users Functional Manager for unlocking and enablement
- e. In case a user going on leave for a period of more than 30 days, then the respective users functional manager shall inform location IT department for disablement of the user ID during that period and enable the User-id when the user resume work and approved by functional manager.
- f. User accounts which have not logged into the systems/application for more than 90 days shall be reviewed and disabled by the IT department based on approval from Head of Department (HOD) or CIO.

9.4 User ID Security controls

- a. The User IDs/accounts shipped along with software and hardware shall be disabled.

- b. Users logging into domain application for authentication, with entering wrong passwords Five times should result in user's account being locked. The Domain systems to be configured for automatic unlocking of users within half an hour.
- c. Applications which are not integrated with domain for authentication, Users to contact IT department for unlocking the user id and resetting the password.
- d. Desktops/laptops should be set to auto lock after Twenty minutes of inactivity. These shall unlock using User's login id and password.
- e. IT department shall ensure Servers desktops; Laptops and Network devices have accurate setting of computer clocks to ensure accuracy of audit logs, which is required for investigations or as evidence in legal or disciplinary cases, and Users shall not be able to change clock settings.
- f. Users shall have a dedicated shared drive configured for storing the critical business data.

10. ERP Applications Security Policy

10.1 ERP Applications Access Management

- a. User's access and the role privileges to the ERP systems shall be approved by functional manager/Head of Department (HOD) & CIO and request to be forwarded to the IT department.
- b. Post approval IT department shall create User ID and grant access to the ERP Roles, menus and programs.
- c. The ERP access to respective programs and Menus shall be granted based on defined and agreed "User Authority Matrix.
- d. Any change in Users role access shall be controlled and managed through User Authority Matrix to ensure access compliance with respect to the role of the user.

10.2 Access to Legacy ERP Systems

- a. As per the business requirement Users shall have access to legacy ERP systems and applications for executing the task till all existing business processes is migrated to the new ERP systems.
- b. Any new User ID creation and grant of access to the legacy systems shall be restricted to view access and shall be approved by the respective functional manager or the Head of Department (HOD).
- c. The approved Request details of legacy systems shall be maintained by IT department for future reference and audit purpose.

10.3 Customization of Applications

- a. Customization includes enhancement/modification on the existing ERP application.
- b. Customization requirements should be reviewed and approved by the functional Manager/Head of department (HOD) and to be submitted to the IT department for relevant action.
- c. The IT department may use resources within organization or would engage third party consultants for executing the required customization work.
- d. The IT department shall maintain documentation and record of all approved customizations carried out on the applications, along with Source Code.
- e. Audit trail's to be enabled for certain business required fields to check and track the transactional value changes and for the purpose of investigation in case of any fraud.

11. Password Management Policy

11.1 User Password management in Active Directory Domain Services

- a. The password selected should be combination of alphanumeric with special character and at least one character in capital and one in small alphabet.
- b. Length of password shall be minimum 8 characters.
- c. System to enforce user-level passwords change at least every 90 days (e.g., email, login to desktop, laptop etc.)
- d. 3 last passwords shall not be used again. System should remember last 3 passwords.
- e. Account lockout criteria shall be set for 5 unsuccessful login and disclaimers for users shall be displayed like "Account locked".
- f. System should enforce change of password at first usage of the initial password. The IT administrator while creating the user-id shall enable "Force Password Change at First Logon".
- g. Users shall be notified to change their password 10 days prior to expiry. System enforced message shall be sent to users warning them about the account lockout in case they fail to change their passwords.
- h. In case of Account unlock or for any change of password to a new one Users to contact IT department and get this actioned.
- i. Passwords should not be stored in readable form in batch files, automatic logon scripts, Internet browsers or related data communication software, in computers without access control, or in any other location where unauthorized persons might discover or use them.
- j. The "Remember Password" feature of applications should not be used.

- k. If the password is shared with support personnel for resolving problems relating to any service, it should be changed immediately after the support session.
- l. For password change, both old and new password are required to be given.

11.2 Privileged/Super User Password management

- a. Privileged or administrator User-id password shall only be used to perform any system and configuration changes and shall be approved as per change management policy.
- b. Users shall not be granted with administrator access to execute and day today operational transactional activities.
- c. All Systems/applications privileged/administrator User Id password to be vaulted
- d. IT department to ensure all Systems and applications Privileged/administrator passwords are changed to ensure these remain active at all times.

12. Anti-Virus Policy

12.1 Deployment of Anti-Virus Software

- a. IT Assets across LNJB group either in the Data center/Server rooms or other hosted environment are to be kept updated with latest antivirus software at all times.
- b. In order to ensure consistency in updating of the antivirus software across the group, the same has to be deployed centrally.

- c. In order to protect IT Assets from Virus attack, the centralized updating system should be configured such that all IT assets are updated with latest Anti-Virus patch in shortest possible time.
- d. IT department shall ensure for Users desktops, Laptop's which are not updated automatically are to be manually configured with latest Anti-Virus software and reconcile the status update by verifying at Antivirus server Console.

12.2 Managing Anti-Virus software installed on IT Assets

- a. Controls shall be in place to restrict Users from disabling the Anti-Virus Software installed across LNJ Bhilwara group.
- b. All IT systems across LNJ Bhilwara group shall be configured to run regular virus scans across all data files to detect and cure a virus.
- c. Anti-Spam, Antivirus device shall be configured to filter out email spams and malicious content before reaching the users mail box.
- d. Any IT system infected with Virus shall be removed from the network until they are verified as virus-free.

12.3 Recommended best practices for prevention from any Virus Threat

- a. Users shall not forward spam/chain/junk email as they may contain viruses.
- b. Users shall not open any files, unknown link/url or macros attached to an email from an unknown, suspicious or untrustworthy source.
- c. Respective location IT Heads shall have access to antivirus console to check and fix Anti-Virus on compliance issues with respect to their location.
- d. IT department shall make users aware of the potential threat of viruses and the various mechanisms through which they propagate and accordingly the Users must be trained not to open attachments/unknown links/urls unless they are expecting them.

- e. For tracking any unauthorized access attempt or virus issue, Antivirus server should be configured with at least 30 days logs.

13. Software License Management Policy

13.1 Software License Procurement, Distribution and Usage.

- a. All Software Licenses purchase, deployment, removal & retirement across LNJB are to be accounted by respective IT department so as to ensure compliance at all times.
- b. Before installing any software IT department shall ensure that it's not always that the presence of particular software on a user's prior system(s) shall be the criteria to have that software installed on a new or replacement computer for that user rather the software shall be installed based on the business requirement.
- c. Users across the group shall adhere to copyright laws and packaged Software License agreements. Users violating the copyright laws in any way either by acquiring, storing or loading a pirated license will be singularly responsible for this misconduct and will face severe disciplinary action.
- d. Software's Licenses required for LNJB group business functions shall be procured centrally.
- e. All details with respect to Software License date of purchase, License type etc. shall be maintained by the IT department.
- f. Any Software Licenses purchased by respective location IT department in urgency to meet urgent need of business are to be informed at corporate office.
- g. All licensed software's shall be stored at safe location and access shall be only to relevant IT team member authorized to install at Users computers.

13.2 Managing Software Licenses

- a. The software license is to be tracked and reported by location IT to Corporate IT such that all units comply with License contract.
- b. License key being confidential information to be safe guarded and to be shared only to authorized IT Team members.
- c. The inventory of existing software licenses shall include (product name, version, type of license, expiration date and proof of purchase.
- d. Software Licenses procured by the organization shall be reconciled by the IT department against deployment and ensure compliance across all units.

13.3 Use of Evaluation software, Open source software and Freeware

- a. Basis business requirement the IT Department will get the evaluation software, freeware or open source software (OSS) through product site or from local authorized service partner.
- b. The evaluation software is to be tested for any Virus or malicious content before it's installed on the Users system.
- c. IT department shall maintain a record with details of "Name of the computer, Username, name of the evaluation software, date of installation and date of expiry of the evaluation software.
- d. IT department shall ensure evaluation software's are uninstalled from the computers once the evaluation is completed by business users.
- e. Organization decision to go for licensed software or Open Source Software or Freeware shall be based on the Organization compliance, project requirement, and cost of the software, scalability and ROI.

- f. All customization done using the Open Source Software (OSS) /freeware shall be documented and stored as a repository at a secure location for necessary debugging and future audit purpose.

13.4 Reporting and Tracking of Software Licenses

- a. IT departments shall undertake Quarterly License compliance check of only critical business applications against total number of license procured and deployed and any discrepancy to be corrected within 24 hours.

14. IT Help Desk Management

The purpose of the IT Helpdesk management is to provide a frame work for dealing with Incidents and service requests related to IT Assets, applications and infrastructure.

14.1 Logging of Issues/Incidents.

- a. Across the organization Users shall have access to IT service management tool to report Issues with respect to IT incidents.
- b. Based on the issue reported by the users the IT department shall check and provide resolution within the agreed time lines as per the SLA.
- c. Plant IT Heads shall review incidents and service requests logged with respect to their location and ensure no tickets /issues reported breach the defined SLA.
- d. All configuration/design changes within the IT Service management tool shall be managed by IT department at Head Office

14.2 Incident reporting, resolution and monitoring

- a. Based on Users incident reporting, respective location IT department shall address the issues and provide timely resolution.
- b. Location IT Head shall periodically monitor all the calls/tickets which have not been resolved within the stipulated SLA and escalate to relevant support team for necessary resolution.
- c. Corporate IT department shall publish Monthly compliance report to CIO for review and monitor the issues reported and closed by all locations
- d. Calls logged/ Security incidents shall be resolved according to the timeframes below.

Call/Incident Severity	Response Time	Resolution Time
Urgent	15 Mines	1 hr.
High	45 Mines	2 hrs.
Medium	1 Hr.	3 hrs.
Low	1 Hrs.	4 hrs.

15. Backup & Restoration Policy

The objective of backup policy is to ensure protection and retention of as recent data as required by business such that same can be retrieved within the time specified by the business user of that application in the event of any disaster. The frequency of data backup should be in sync with criticality of that data such that there is no loss of data. This business requirement of as recent backup as possible & as quick restoration as possible need to be balanced with the infrastructure

required to take backup at the defined frequency and restore as quickly as required by business.

15.1 Data Backup criteria

- a. Users shall store all business critical data files at the designated locations on the common file server, as provided by IT department.
- b. IT department shall maintain details of all critical servers, applications & Databases for which a regular backup is required.
- c. Backup shall be scheduled as Daily incremental and Weekly full back up or as defined by business application owners. The Data and system files that are backed up shall be sample tested for successful restoration at least once a month.
- d. Adequate corrective measures to be taken for any discrepancies or errors found during the backup testing. Avoid similar discrepancies in future.
- e. Backup of all ERP Database and e-mail must be retained such that all systems are fully recoverable (with as recent data as pre-agreed with respective business application owners). This may be achieved by using a combination of different cartridges/media with full, incremental, or other techniques but within the pre-agreed time frame.
- f. At any point in time a maximum of 30 days data to be made available in the Storage area network (SAN) box.
- g. At a minimum, one fully recoverable version of all the complete and as recent data as pre-agreed shall be made available and must be stored in a secure, off-site location.
- h. IT department should ensure backup media of database (of as recent data as per business requirement) is maintained at an offsite location in a secured fire-

rated cabinet and moisture-free environment and preferably at a different & far location from Data Center.

- i. Configuration files of firewall, switches, routers etc. shall be backed up in order to retrieve these during hardware failure.
- j. The backup media must have label as per labeling convention e.g. Backup type, date etc. The Backup media shall be erased/ zeroed before sending for repairs, disposal for preventing retrieval of any data from such media. And these media shall be destroyed post expiry of the retention period.
- k. All offline/ archived information should be made available to the authorized user/ regulator or any other statutory authority when requested. Access to the archived data shall be provided after the written approval of concerned Head of Department (HOD) & Business Head.

15.2 Data Backup management

- a. Centralized Backup: Applications & Databases hosted at corporate locations which are used by users across LNJ Bhilwara group the data backup are configured and managed at a central location. Backup configured and managed centrally:
 - i. Full Virtual Image backup of critical Servers.
 - ii. ERP application and Database backup of all companies.
 - iii. E-mail database
 - iv. Antivirus EPO data base and Virtual image
 - v. Domain controller active directory database
 - vi. Business intelligence application & Database
 - vii. User data residing on corporate location File Server
 - i. Backup of any specific data as informed by Business owners

- b. Data backup at Plant locations: Backup of applications & databases hosted at plant locations and used by respective location users. Backup to be configure and managed for:
 - i. User data residing on location File Server
 - ii. Critical Server Virtual image backup
 - iii. Any location specific hosted applications & Database
- c. The 3-2-1 rule of backup detailed below may be considered:
 - I. IT Department must have at least three copies of data: the original production data and two backups.
 - II. IT Department must use at least two different types of media to store the copies of data (eg. local disk, tape and external hard disk).
 - III. IT Department must keep at least one backup offsite (in the cloud or in a remote site).

15.3 Data Backup frequency: Backup to be configured as:

- i. Daily incremental backup to be configured on a storage device for each of the applications, user data separately. Weekly full backup to be configured on a storage device for each applications and User data separately
- ii. The Backup data to be retained for a period of 30 days in the storage device. Monthly backup of complete Virtual image of Operating system and application configuration to be copied on an external media/Tape and stored at offsite location.
- iii. Daily full backup to be performed for Critical ERP database on a Tape media and data to be stored at offsite location at least twice weekly to ensure business continuity.

- iv. Based on any changes in the existing infrastructure server or database configurations, the Backup frequency shall be reviewed and updated by the IT department to ensure there is minimum business disruption

15.4 Restoration

- a. A request with approval from functional manager/Head of department shall be forwarded to the IT department for any restoration requirement.
- b. The respective unit IT department shall be responsible for restoring the data/system from the backup tapes/media/storage device and shall log/record all the activities (i.e. details of the file, username, time of restoration & success or otherwise of restoration exercise etc.) for future tracking and audit purpose.

15.5 Removable Media Disposal

- a. The Media containing business information shall be destroyed before disposing them.
- b. Magnetic media shall be securely formatted or the media shall be degaussed before disposal.
- c. All disposals of sensitive media shall be recorded for audit trails.
- d. All backup cartridges/media that are not re-usable shall be thoroughly destroyed and destruction certified placed on file for audit and record.

16. Data Classification policy

Information shall be disclosed only to those people who have a legitimate Business need for the information and the data classification scheme shall be designed to support the “need to know” policy so that information will be protected from unauthorized disclosure, modification and deletion.

16.1 Identification and Inventory of Information Assets

- a. Business Units to identify Information Assets, their location, Usage and business criticality.
- b. The assets of LNJ Bhilwara group includes:
 - i. **Information:** Databases, Contracts and agreements, Policies, Procedures, Data Backups, source codes etc.
 - ii. **Software:** Operating systems, Application Development tools, Utilities
 - iii. **Hardware:** Desktops, Laptops, Network Assets,
 - iv. **Personnel & Services:** People, Outsourced services,

16.2 Data Classification Matrix

- a. Across LNJB group companies four –level of information classification shall be followed (**Restricted, Confidential, Internal & Public**).
- b. Based on the information classification as notified by the respective business owners, IT department shall deploy controls and ensure this information is secured.

Data Classification Matrix Definition and examples

Classification	Definition	Examples
----------------	------------	----------

Level		
Restricted	This classification applies to the most sensitive Asset, which is intended strictly for use within LNJ Bhilwara group companies and Its unauthorized access could seriously and adversely impact organization, its stockholders, its business partners and/or its customers leading to legal and financial repercussions and adverse public opinion.	Merger and acquisition plans, planning for existing litigation, trade secrets, customer data and information security data, Strategy Documents. NAT and routing details.
Confidential	This classification applies to less sensitive Assets, which are intended for use within LNJ Bhilwara group and Its unauthorized access could adversely impact LNJ Bhilwara group, its stockholders, business partners, employees and/or customers.	Internal audit reports, Procedures, Short-term marketing plans, analyses of competitive products, knowledge, skill and information of LNJ Bhilwara group and its people.
Internal	This classification applies to Assets, which are generally accessible to LNJ Bhilwara group employees. The access to such information/asset may be through a unique authentication or may be accessible through the privileges of being an LNJ Bhilwara group employee. While its unauthorized Access/ disclosure is not expected to seriously or adversely impact LNJ Bhilwara group employees / customer's stockholders & business partners.	LNJ Bhilwara group telephone directory, training materials and policy manuals. Common Intranet information
Public	This classification applies to information, which has been explicitly approved by LNJ Bhilwara group management for release to the public	Service brochures, advertisements, job opening announcements and press releases

16.3 Data Classification rules

- a. The classification of any Asset shall be determined based on the Confidentiality, Integrity and Availability of the asset.
- b. All employees across the organization should be aware of the data classification matrix and shall take necessary precautions while handling sensitive information at all times.

16.4 Declassification / Downgrading

- a. Based on the value of information, the designated information owner shall, at any time, declassify or downgrade information. By changing the classification label appearing on the original document.

16.5 Managing Data Confidentiality

- a. The Head of department and users within each department shall be responsible for managing the confidentiality of respective business data and will seek support from IT department to ensure data confidentiality.
- b. Users shall not use the organization IT infrastructure, application and communication systems, whether standalone or in conjunction with any other device, to make an unauthorized disclosure or copy of confidential information belonging to the Group/Company.
- c. Unauthorized disclosure information belonging to the Company will be liable for appropriate disciplinary action.
- d. Confidential information shall include details of:
 - i. Business contacts, associates, lists of customers.
 - ii. Suppliers and details of contracts with them.
 - iii. Tenders, projects, acquisitions etc.
 - iv. Employee details and their remuneration.
 - v. Sales, expenditure and buying/pricing policies.
 - vi. Proposals, plans or specifications for the development.
 - vii. Accounts, trading statements, statistical information.
 - viii. Corporate and marketing strategy, business development.
 - ix. Financial, sales, reports and research results.

17. Incident management policy

17.1 Incident management practice standard

- a. Within LNJB group all IT and Security related incidents shall be handled by the IT department.
- b. Whenever a security incident, such as virus, worm, fake email, discovery of hacking tools, any altered data interference in communication etc. is suspected or confirmed, the appropriate incident management procedure as stated below must be followed appropriate Incident Management procedure as stated below must be followed.
 - i. IT department should be notified of such security incident through a mail, call or through IT Service management tool by logging an incident.
 - ii. Within IT department the respective identified team/person would be responsible for analyzing, initiating the appropriate incident management action including restoration, as per established guidelines.
 - iii. The Security incident response and resolution time depends on the nature of the incident and would be same as defined in section 14.2.d
 - iv. The IT department shall ensure that any damage from a security incident are repaired or mitigated and that the vulnerability is eliminated or minimized where possible.
 - v. The Head of department/CIO shall report the incident to the management and also share communication to Users through mail.
 - vi. Post resolution the root cause analysis and corrective action details shall be documented and shared by the respective team/person to CIO and other relevant teams to safe guard against any such similar incidents in future.

18. IT Planning Budgeting Training & Skill development

18.1 Annual IT Budget planning

- a. Annual IT budget shall be planned and finalized by Corporate and location IT department before the beginning of financial year and must include both capital and operational expenses.
- b. Corporate IT shall share the split IT expenditure details to each plant location against the usage of Common applications, utilities, Tools, licenses and other services which are used by users across the plant locations.
- c. Respective location IT Head shall collate the IT expenditure inputs as received from corporate IT department and in-corporate this along with plant location specific IT expenditure while preparing the final annual IT budget.
- d. The final IT budget of each location shall be submitted to Location Head/Business Head for integration with overall budget for the Location and necessary approvals.
- e. IT Head of respective location shall communicate the details of final approved annual IT Budget to Corporate IT department /CIO.
- f. In case of capital expenditure, the tangible business benefits must be evaluated in planning stage and possible consent of related business head/HOD is to be attached.

18.2 Unbudgeted IT Expenditure:

- a. For any exigencies or any expenditure pertaining to immediate requirements for IT to cater to major unforeseen issues affecting business operations or for any new un-planned technology projects or hardware requirement, the approval for the same shall be obtained from the respective location Business

Heads on a case-to-case basis by the Location IT Head in discussion with the corporate IT Department/CIO.

18.3 Training & Skills Up gradation

- a. A yearly training plan for IT department shall be identified and accordingly budget to be approved.
- b. The skill-sets of IT Team members across the Group shall be mapped against the projects and new technology and the gaps identified to be plugged with suitable training.
- c. IT department shall plan and execute awareness training for Business users on various IT security practices and ensure users are made aware of do's and don'ts which each user shall be aware of including data protection, data classification, access control and general security threat, social engineering threats like fishing & other common cyber-attacks.
- d. Clean desk policy: Laptops should be taken home and documents shouldn't be left on desks at the end of the work day.

19. Change Management policy

19.1 Scope of change management

- a. The change management policy applies to all changes to the following areas:
 - i. Operating systems changes, which must include service packs, configuration changes and version upgrades.
 - ii. Changes to applications, which must include application of patches, configuration changes and version upgrades.
 - iii. Changes to networks and network devices like routers, switches, firewall, etc. This must include changes to router & switch

configurations, IOS, firewall policy changes, network layout/traffic changes.

- iv. IT hardware changes such as change of RAM, CPU and HDDs etc.
- v. Additions of new application/new Hardware to the existing setup.
- vi. Relocation of systems from one location to another location or application movement to a different server/location.

19.2 Change Management and Documentation

- a. Any changes to the system must involve documenting and managing the change requests.
- b. The documentation should contain brief description of the changes requested, the date on which the request was made, prioritizing of the request, tracking and controlling modifications and assigning a unique number to each request.
- c. All changes must be scheduled and all the affected parties must be informed in advance of the change.
- d. All Change Request initiated as per the standard change request procedure and shall be evaluated by corresponding module owners and further approved by the CIO before implementation.
- e. All changes have to be reviewed after the roll out.
- f. Post-implementation reviews shall be performed for the critical IT solutions developed to assess whether the system delivered the benefits envisioned in the most cost efficient and effective manner.

19.3 Change approval

- a. Based on the business requirement the respective business function data owner shall submit the change request form duly approved by the respective functional manager/Head of Department.

- b. An assessment of the proposed system changes must be performed to assess its potential impact on LNJB systems before its approved
- c. This approved change request shall be forwarded to the IT department and based on the changes as classified as Normal/Emergency the IT department shall execute the change request and provide confirmation.

19.4 Testing of Changes and Backup










- a. All changes must be tested before being carried out in the live/ production environment, wherever required.
- b. A backup of the system impacted by the change must be made prior to it being updated.
- c. A roll back procedure should be in place to revert back in case the changes deployed in the production fail to derive the desired result.











19.5 Unscheduled/emergency changes





- a. All Unscheduled/emergency changes must be carried out only in case there are critical production issues, which require the change to be carried out.
- b. Approval shall be obtained to execute the unscheduled/emergency changes.
- c. Post the execution of emergency changes all required documentation with respect to emergency change must be in place for future reference and audit purpose.
- d. An audit trail of the emergency activity must also be generated which logs all activity as stated below:
 - i. The user-ID making the change
 - ii. Time and date
 - iii. The commands executed
 - iv. The program/menu/data files which will be affected.

Annexure /Forms

Attached here with are the Templates and forms available in softcopy copy against various sections of the policy for record keeping as per the requirement/need.

S. No	Description	File
1	Asset Issue Receipt Section 4:-IT Asset Life Cycle Management Policy	 Ref 1_ASSET ISSUE RECEIPT.doc
2	Record of IT Assets Section 4:-IT Asset Life Cycle Management Policy	 Ref 2_Record of IT Assets.xlsx
3	IT Asset Allocation Sheet Section 4:-IT Asset Life Cycle Management Policy	 Ref 3_IT Asset ALLOCATION SHEET.
4	e-waste Log Section 4:-IT Asset Life Cycle Management Policy	 Ref 4_E-waste.xlsx
5	User id creation for applications and email	
A	User Access Rights Form for TIM	Ref 5_TIM Profile Creation request form
B	User Access Rights Form for BPCS	
C	User Access Request form for E-mail, Internet, Systems and applications and M3	Ref 6_BPCS request form.xlsx
D	M3 User Access request form: Ref R-10	
E	User Access Request Form Using IT Service management tool Sapphire- Ref: R-11	Ref 7_R-09-User Access Request Form
		
		Ref 8_M3-User Access Request Form
		
		Ref 9_User Access Request_ITSM Sapph

F G	NOW User Access/Profile Request Form SAP User Access /Profile Request form Section 7, 9:- Email Access & Access control Policy	 Ref 11_NOW Profile Creation request form  Ref 12_SAP request form.docx
6 A B	Change Request Form & Guidelines for Change management request to be raised through ITSM tool Section 19:--Change Management Policy	 Ref 10_R-19 Change Request form_Update  Ref 18_SOP of Change management
7	Record Retention Schedule Section 16:-Data Classification Policy	 Ref 13_Record retention details.xlsx
8 A B	Service Request Form Section 14: --IT Helpdesk Management Incident and Service Raising using IT Service Management Tool Sapphire Section 14: --IT Helpdesk Management	 Ref 14_Service request form physical  Ref 22_Raising Incident request thro
9	Applications Functionality Control (Indicative for TIM/BPCS, similarly for other Applications)	 Ref 15_AS00 Functional Control.xls
10	IT Dept Compliance SOP and Control check list for Employee Exit.	 Ref 16_SOP ITdept Compliance chk for er  Ref 17_IT Dept Compliance Checklist

11	IT Asset Destruction certificate and IT Asset disposal process	 Ref 19_IT Asset destruction Certificat  Ref 23_D-04 IT Asset disposal proces
12	Applications and database backup Matrix Section 15:- Backup and Restoration Policy	 Ref 21_Data Backup Matrix HO NOIDA_up
13	ERP Application and Data base details of RSWM, Maral and HEG Section 10:- ERP Application Security Policy	 Ref 20_ERP Application details_LN

CONFIDENTIAL