IT SECURITY POLICY FOR NANDAN DENIM LIMITED

An IT Security Policy, also known as a Cyber Security Policy or Information Security Policy, sets out the rules and procedures that anyone using a NDL's IT system must follow.

The policy includes guidance regarding confidentiality, system vulnerabilities, security threats, security strategies and appropriate use of IT systems. It will also make it clear who is responsible for various security measures and explain what should happen if there is a security breach.

NDL IT Security Policy advises of the potential consequences if employees fail to adhere to the policy.

1. Objectives

This policy and the framework are designed to:

- Promote a holistic approach to information security management.
- Protect NDL's information and technology against compromise of confidentiality, integrity and availability
- Support NDL's strategic vision though an approach which effectively balances usability and security
- Facilitate "security aware" culture across organization and promote that information Security is everyone's responsibility.

2. Scope of the Policy

The scope of this Information Security Policy covers the storage, access, transmission and destruction of information in the course of NDL business. It therefore applied to the conduct of employees and others with access to that information (wherever the information or they are located) as well as the applications, systems, equipment and premises that create, process, transmit, host or store information whether in house, personally owned or provided by external suppliers.

3. Governance

The responsibility for the production, maintenance and communication of this top level policy document and all sub policy documents lies with Head – Information Technology.

This top-level policy document has been approved by the CEO. Substantive changes may only be made with the further approval of CEO.

Each of the documents constituting the Information Security Policy will be reviewed annually. It is the responsibility of Mr. Naresh Jain, Head (IT) to ensure that these reviews take place and the policy set is and remains internally consistent.

4. Policy Enforcement

The enforcement of the security policy is responsibility of Mr. Naresh Jain, Head (IT) in coordination with Network team.

5. User Responsibilities

Users are responsible for protecting NDL's information and technology systems and for complying with this policy and the framework. If a user suspects or discovers any material breach of the requirements detailed within this Policy, they must report this to Helpdesk. Where an individual user suspect's personal data may have been compromised, they must notify this to Helpdesk.

6. Messaging Security

6.1 All incoming emails are scanned for viruses, phishing attempts and spam.
6.2 Messaging service include appropriate logs and encryption of data in transit.

7. Acceptable Use of the Internet/Social Media

Employees should not use their email addresses on their private social media accounts as this may compromise the security and privacy of the email system. The exception to this requirement is where accounts are used for interaction for official purpose.

8. Data Encryption

The most of applications are accessed vis HTTPS using Transport Layer Security (TLS). TLS is a cryptographic protocol designed to protect information transmitted over the internet, against eavesdropping, tampering and message forgery.

9. Anti-virus Software / End Point and Server Security

The IT department carries out regular vulnerability assessments, system scans, patch management, threat protection technologies and scheduled monitoring to

identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.

The IT department shall ensure that the company uses an up to date reputable antivirus checking software tool to check the IT systems and to scan all email attachments before they are opened.

Users shall permit any such files to be scanned for viruses as part of the download process. The external storage devices are also scanned for vulnerabilities before allowing access to the content.

The IT department has implemented network security controls that provide for the use of enterprise firewalls, intrusion detection and prevention systems and other traffic and event correlation procedure designed to protect systems from intrusion and limit the scope of any successful attack.

10. General Software

All software installations on the IT System shall be the responsibility of the IT department. All software installed on the IT systems shall be kept sufficiently up to date in order to ensure that the security and integrity of the IT systems in not compromised.

11. Physical / Hardware Security

All company mobile devices (including without limitation. Laptops, iPads and mobile telephones) should be kept securely by Users. Users should not leave such mobile devices unattended other than at their homes or Company premises.

Users are not permitted to connect any of their personal hardware to the IT System without express approval of the IT department in writing.

12. Working from Home / Remote Working

Users must note that when using home PCs or other equipment at fixed locations outside the office, they are operating outside the Enterprise IT Security perimeter.

It is the responsibility of the users to ensure that PCs used for home working are themselves properly secured. Weak security on home PCs used for home working could lead to the compromise of their account and result in security incidents involving Enterprise IT systems.

Users are responsible for the safeguarding of equipment against unauthorized access, misuse, theft or loss when in their home or in transit. Where home computers are used by other family members, no organizational information should be accessible by such unauthorized parties.

Users must ensure that all reasonable protection measures are in place and operating where applicable as follows:

- The computer's local firewall should be enabled
- Antivirus software should be installed and set to automatically update itself.
- Up to date security patches should be installed for both the Operating System and applications when released by software vendors and set to automatically update itself.
- Wireless networks at home must be properly secured against eavesdropping and intrusion.

Users must comply with the security requirements of this document at all times and where personal data is being processed, they must also comply with the Employee Appointment Letter

Users must not access internal or confidential / sensitive information over unsecured broadband or public wireless networks as these present a security risk. Users should also be aware of the physical environment when working remotely ensuring no one is looking over their shoulder at information on screen.

13. Responding to Security breaches

As in all cases of security while the company endeavours to do everything it can to prevent the attacks and outcomes described, the preventative measures are not always successful. In the case of a successful attack being perpetrated the following steps will be taken in each case.

Data loss (deleted from the active system)	**Data will be restored to the active system using one of our backups.**
Data integrity breach	Data on the active system will be compared to back up data and overridden with the backup data if change is suspicious.
Data theft	The organizations affected by theft of the company data will be informed as soon as possible with advice on what they should do to protect themselves from the stolen data being used against them.
Virus / malware detection	Attempts will be made to establish what the virus/ malware is, what it is doing and where it came from before being removed.
Physical theft / Damages	Equipment will be replaced as soon as possible to prevent disruption to the operation of the business.

In any case of breach of security, the root cause will be found and steps put in place to prevent the same kind of breach happening again.

14. The IT Security Tools details are as under –

End Point Protection - Deployed endpoint protection suites from SEQRITE for PCs and Laptops. All endpoints are designed to get automatic updates from eScan server as and when a new definition is released. A Central Console is available for monitoring assets installed at various locations including alerts/ warning on email for timely actions.

Server Protection – All agents are configured for automatic updates from SEQRITE server as and when a new definition is released. A central console is available for monitoring status of all servers including alerts and warnings for timely actions.

Firewall – Server rooms are equipped with Fortiget 100/Sonic Firewall with High Availability (HA). Inbound and Outbound Traffic are being filtered via Firewall which is bundled with IPS & IDS. De-militarized Zone has been created for Servers. Internet Gateway, Wi-Fi are secured with Firewalls.

Email Security – Email server is hosted at Chiripal House on premise with required engine for scanning of emails for identifying and removing suspicious emails. Users are accessing email services over Mobile devices which is secured with TLS/SSL.

Remote Access – We are configuring secure VPN / VPN Site to Site tunnel to allow access to our applications and network for remote access from locations where we do not have MPLS connectivity or MPLS link is down.

Undertaking from Employees – All employees have provided an undertaking on authorized usage of IT Facilities and applications including protection of confidential information. We have exhaustive Induction program for New joiners / Trainees in which information pertaining to IT Security is covered. In case of incidents related to Ransomware, Email Spoofing, Virus threat etc. all employees are communicated by Email for practicing necessary caution.

The responsibility matrices are as under –

IT System	Tools	Person Responsible for Monitoring and Resolution
End Point Protection	SEQRITE End Point	Mr. Mohsin/Jayant- Admin
Server Protection	Firewall and SEQIRITE	Mr. Mohsin/Jayant – admin
Firewall	Fortiget 100	Mr. Mohsin/Jayant – Admin
Email Security	Firewall and SEQIRITE	Mr. Mohsin/Jayant/Paras
Remote Access	Firewall /VPN	Mr. Mohsin/Jayant- Admin