POLICY OBJECTIVE:

This policy establishes a firm commitment by management and employees to foster a culture of integrity and responsibility in handling personal and organizational data. It aims to embed accountability among stakeholders, ensuring compliance with data protection regulations, safeguarding confidentiality, and promoting transparency in data processing. By prioritizing security, ethical data management, and user privacy, we assure stakeholders a consistently secure and trustworthy experience.

POLICY GUIDELINES:

i. All company data to be collected for specified, explicit and legitimate purposes and to be further processed in a manner that is compatible with intended purposes.

ii. While handling of personal data it must be in line with this policy and data protection principles to always maintain the confidentiality of personal data of persons of concern, even after a data subject is no longer stay in the Company.

iii. Transfer of Personal Data will be done only with necessary consent and only is cases necessary for important public interest reasons or for the conduct of legal claims.

iv. All company staff be granted access to the data and applications required for their job roles. Sensitive systems should be physically or logically isolated to restrict access.

v. Access to data classified as 'Confidential' or 'Restricted' shall be limited to authorized persons whose job responsibilities require it as determined by management.

vi. Accuracy of the Company data is to be ensured and shall be kept up to date.

vii. Data should be kept in a form which permits identification of data subjects and to be stored no longer than is necessary considering the purposes for which that data was originally collected.

viii. Data Responsibilities shall be applicable to everyone who works for or with Company and shall have responsibility for ensuring that data is collected, stored and handled appropriately.

ix. All users must lock their screens whenever they leave their desks to reduce the risk of unauthorized access. All users must keep their passwords confidential and not to share them with others.

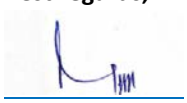
x. Company treats data breaches very seriously and any employee who becomes aware of a likely data breach should immediately inform the Section Head and IT department, failing which shall be subjected to disciplinary actions.

OBLIGATIONS AND COMMITMENT:

NHL Management is committed to implementing and adhering to applicable regulations, ensuring that all work activities align with established quality standards and agreed-upon specifications. Through proactive compliance and structured execution, we uphold excellence in every aspect of our operations.

Policy authorised by:

Best regards,



Mustafa S. Ali
Chief Executive Officer
mustafa@nudooj.com | www.nudooj.com