1 Overview

NRB Information Security Policy shall abide by the core ethos, established organisation culture, mutual trust and integrity and shall no way try to lay upon any restrictions contrary to the above.

NRB's Information Security Policy is committed to protecting its employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

All devices, methods and tools such as laptop/desktop, storage devices, operating systems, software, mailing systems, internet, intranet, file servers, file sharing systems are property of NRB and these systems are exclusively deployed for to be used to conduct business serving the best interest of the company and of our clients and partners / vendors during business operations.

Having the complete knowledge of this Information Security Policy and the guidelines therewith is responsibility of every computer user / information user and an effective implementation of policy solely depends on the entire team's involvement, participation and support by way of imbibing the laid out policy in letter and spirit while conducting their business activity accordingly.

2 Purpose

The purpose of this policy is to layout acceptable use of all IT means and methods such as Laptop/Desktop or other equipment and electronic device/s, these rules are to protect the employee and NRB. Inappropriate use exposes NRB to cyber risks including virus attacks including ransomware, compromise of network systems and services, data breach, and legal issues.

3 Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct NRB business or interact with internal networks and business systems, whether owned or leased by NRB, the employee, or a third party. This policy applies to all the employees, contract workers, partners, suppliers, customers, third-party and their employees who have access to NRB premises, systems and information to exercise good judgement regarding appropriate use of information, devices and resources in accordance with this policy, standards and local laws.

4 Policy

4.1 General Use and Ownership

4.1.1 NRB proprietary information stored on electronic and computing devices whether owned or leased by NRB, the employee or a third party, remains the sole property of NRB. You must ensure through legal or technical means that proprietary information is protected always.

4.1.2 You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of NRB proprietary information.

4.1.3 You may access, use or share NRB proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

4.1.5 For security and network maintenance purposes, authorized individuals within NRB may monitor equipment, systems, and network traffic at any time. Information collected during monitoring shall not be of anything personal in nature, however the information collected shall be purely to ascertain any potential misuse of the information, unethical distribution of information beyond permitted boundaries, unauthorized attempts to obtain information by electronic means, track and trace alerts raised by tools such as Antivirus and also based on the inputs from the SOC (Security Operations Center) team

4.1.6 NRB reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.1.7 Policy Awareness: All users shall be part of Information Security Awareness program in the form of email campaign, organized workshops, knowledge sharing sessions.

4.1.8 Separate "Risk Managemen Frame work" shall be created and published which will address key areas such as identification of risk both current and potential, methods to mitigate the risk.

4.1.9 Incident Response Plan shall be necessitated by means of deploying relevant security solutions such as Antivirus, Firewall, Data Encryption tools, EDR (Endpoint Detection and Response) tools which helps in both incident detection and remediation

4.2 Security and Proprietary Information

4.2.1 All mobile and computing devices that connect to the internal network shall be governed by access policy which will be in force and amended time to time.

4.2.2 System level and user level passwords must comply with the *Password Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.3 All computing devices must be secured with a password-protected lock screen with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

4.2.4 Postings by employees from a NRB email address to newsgroups or other online platforms, should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of NRB, unless posting is during business duties.

4.2.5 Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of NRB authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing NRB-owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by NRB.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which NRB or the end user does not have an active license is strictly prohibited.
3. Accessing data, a server, or an account for any purpose other than conducting NRB business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, trojan horses, ransomware, etc.).
6. Revealing your account password/passphrase to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
7. Using NRB computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any NRB account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is notlimited to, network sniffing, ping floods, packet spoofing, denial of service, brute-forcing accounts, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless prior notification to the Infosec Team is made.
12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

13. Circumventing user authentication or security of any host, network, or account.
14. Introducing honeypots, honeynets, or similar technology on the NRB network.
15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
17. Providing information about, or lists of, NRB employees to parties outside NRB.

4.3.2 Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone, text, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within NRB's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by NRB or connected via NRB's network.
7. Posting the same or similar non-business-related messages to large numbers of users (group spam).

4.3.3 Blogging and Social Media

1. Blogging or posting to social media platforms by employees, whether using NRB's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of NRB's systems to engage in blogging or other online posting is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate NRB's policy, is not detrimental to NRB's best interests, and does not interfere with an employee's regular work duties. Blogging or other online posting from NRB's systems is also subject to monitoring.
2. NRB's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any NRB confidential or proprietary

information, trade secrets or any other material covered by NRB's Confidential Information policy when engaged in blogging.
Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of NRB and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by NRB.

3. Employees may also not attribute personal statements, opinions or beliefs to NRB when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly, or implicitly, represent themselves as an employee or representative of NRB. Employees assume any and all risk associated with blogging.

Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, NRB's trademarks, logos and any other NRB's intellectual property may also not be used in connection with any blogging or social media activity

4.4 Independent Verification

NRB will conduct VAPT (Vulnerability and Penetration Test) once every year to verify the IT Security setup and preparedness.

5 Policy Compliance

5.1 Compliance Measurement

The Infosec Team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.1.1 Exceptions

Any exception to the policy must be approved by the IT team in advance.

5.1.2 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action as initiated by the management.

6 Oversight on Cybersecurity Strategy and Reporting Mechanism

CIO / Head IT shall be responsible for overseeing cyber security, any cyber security complaints shall be directed to CIO/ Head IT who shall be authorized to initiate appropriate steps in line with Risk Management and Incident Response Plan.

Amendment Record:

Revision no.	Revision Date	Details of Change	Approved By