**Table of Contents**

Table of Contents

1.Purpose4

2. Policy specification4

2.1 General5

2.2 Information security…………………………………………………………………………………………………………………….…..5

2.3 E-mail/Instant Messaging and Communications Activities…………………………………………….…………..6

2.4 Blogging and social media ……………………………………………………………………………………………….…………….6

2.5 Personnel responsibility……………………………………………………………………………………………………………………6

**DOCUMENT REVISION CONTROL**

REVISION HISTORY

REVIEWERS

| **Name** | **Position** | **Date** |
| --- | --- | --- |
|  |  |  |
|  |  |  |

DISTRIBUTION

| **Date** | **Distributed to** | **Version** | **Distribution Format** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

| **Date** | **Version** | **Approved by** | **Designation** | **Signature** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

APPROVALS

| **Date** | **Version** | **Approved by** | **Designation** | **Approval remarks** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |

**List of Abbreviations**

|  |  |  |
| --- | --- | --- |
| **Index** | **Abbreviation** | **Stands For** |
| I | IT | Information Technology |
| 2 | SLA | Service Level Agreement |
| 3 | IOT | Internet of things |
| 4 | IAS | International Accounting Standards |
| 5 | FDP | Finance Department |
| 6 | ITSM | Information Technology Service Management |
| 7 | NDA | Non-Disclosure Agreement |

**Introduction to Acceptable Use of Information Asset**

The purpose of this document is to define acceptable use of information assets, including information, electronic devices, and network resources at <COMPANY NAME> in conjunction with its established norms, policies, guidelines, already in practice at <COMPANY NAME>.

<COMPANY NAME> provides computer devices and other electronic information assets, and it becomes the responsibility of the user of the equipment, devices, and information, to responsibly maintain the confidentiality, integrity, and availability, within the framework of Information Security policies at <COMPANY NAME>.

Acceptable use of information assets requires the users of information assets to comply with <COMPANY NAME> policies and protect the <COMPANY NAME>.

1. **Purpose**

Acceptable use of Information Assets is a policy that makes users responsible for maintaining the confidentiality, integrity, and availability of its information assets provided by <COMPANY NAME>, for the role, and it is to be used within the framework of Information Security Policies applicable at <COMPANY NAME>.

Information Security shall provide exception to the policy, in advance through <Person name> and <Email>.

1. **Policy Specification**

2.1. General

1. Users of Information Assets shall be responsible for acceptable use of information assets provided by <COMPANY NAME> by <COMPANY NAME> Information Security policies.
2. User of Information Assets shall not use any Information Assets provided for any other purpose as specified in his role.
   1. Information Security Department
3. <COMPANY NAME> Information Security Department authorized personnel shall, for security, compliance, and maintenance purposes, monitor and audit equipment, systems, and network, as per this Policy.
4. Devices that interfere with other devices or users on the <COMPANY NAME> network shall be disconnected.

1. Any Breach of Information Security policies, practices by personnel, or information assets shall be reported to Information Security Team.

1. Users shall be responsible for the security of information assets, including information and all devices, as deemed to be provided and approved by the Management.

1. User shall not share passwords, accounts details, or any other information on Information assets with anyone, including other personnel, families, and friends

* Violation of clause five shall be deemed to be a violation of this Policy
* User of any password is required to adhere to password policy

1. User shall ensure to lock the screen when the information assets are left unattended or not in use, as per clear screen and Clear Desk Policy,

* All devices not in use and unattended shall have automatic activation feature of screen saver activation within XX minutes

1. User shall not take out information asset, paper, electronic, information

* User shall be required to take prior approval of only and information security team.
* Violation of clause 4.6.1 shall be deemed to be a violation of this Policy

1. The following are Prohibited, as per this Policy, User is requested to comply with this Policy in words and true spirit of the Policy, but not limited, including,

* User shall not use <COMPANY NAME> e-mail or IP address that violates <COMPANY NAME> policies or guidelines,
* User devices use information assets, approved, and provided by <COMPANY NAME>, other than for inappropriate use.
* User shall be responsible for the use of information assets.

1. User shall exercise good judgment to avoid any violation of mentioned Policy, or in case he does not know the Policy, in whole or is aware partially, of acceptable usage of the information asset,

* User will refer it to superior or to Information Security team located at <COMPANY NAME>, <Location>
* In case of violation of the Policy, the User is subjected to disciplinary action, as per <COMPANY NAME>/ <COMPANY NAME> Disciplinary guidelines & policies
  1. E-mail/Instant Messaging and Communications Activities
* 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)
* Any form of harassment via email, instant messaging, telephone, or paging, whether through language, frequency, or size of messages
* Unauthorized use, or forging, of the email header information
* Sending /viewing/forwarding racial, sexually threatening, defamatory, or harassing emails/instant messages
* 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
* Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type
* Use of unsolicited email originating from within NHA's networks.
  1. Blogging and social media
* Whether using <Company name>’s property and systems or personal computer systems, blogging by personnel is also subject to the terms and restrictions outlined in this Policy. Limited and occasional use of <Company name> plans to engage in blogging is acceptable, if it is done in a professional and responsible manner does not otherwise violate <Company name>’s policy, is not detrimental to <Company name> 's best interests and does not interfere with a personnel's regular work duties.
* <Company name>’s acceptable use policy also applies to blogging. As such, Personnel is prohibited from revealing any confidential or proprietary information, trade secrets, or any other information classified by <Company name>’s Information security policy when engaged in blogging.
* Personnel shall not engage in any blogging that may harm or tarnish the image, reputation, and goodwill of <Company name> and any of its personnel.
* Personnel may also not attribute personal statements, opinions, or beliefs to <Company name> when engaged in blogging. If personnel express their views or opinions in blogs, they may not, expressly, or implicitly, represent themselves as personnel or representative of <Company name>. Personnel assumes any risk associated with blogging.
  1. Personnel responsibility
* All personnel shall report any security weaknesses, incidents, possible misuse, or violation of any <Company name> policies to <Company email id> (email planned).
* <Company name> personnel shall not attempt to access data, information, applications, or programs contained on <Company name>’s information systems for which they do not have authorization or approval from the owner
* <Company name> personnel shall contact the IT helpdesk Team and ensure that latest version of the antivirus software is installed on their desktop / laptop and that the virus definitions are updated
* <Company name> personnel shall not change the configuration of, remove, deactivate, or otherwise tamper with any anti-virus program and other software that has been installed on systems used by them
* Where the mobile device policy allows use of privately-owned devices (e.g., Bring Your Own Device – BYOD), the related security measures shall be considered including separation of private and business use of the devices. <Company name> personnel shall take reasonable measures to ensure the physical security of the device and security of the business information on the device. NHA shall wipe complete information from the device in case of loss or personnel separating from the organization.