Name of the Policy: **IT Policy**		NAVAYUGA
Policy No: NECL/HR/ITP/	No. of Pages:	
Issue Date:	Rev Date:	

Objective:

To lay down the rules and procedures to govern usage of Company's Information Technology Systems and Resources.

Scope:

The policy is applicable to all employees of NECL, its subsidiary Companies, affiliates and third party contractors using Company IT assets and infrastructure.

Description:

- Employees are provided with a host of Electronic gadgets, Technologies and Services, including Computers, E-Mail, Printing and Internet services. These technologies and services are intended to be used for official/business purposes only and are meant to assist employees in completing job responsibilities as effectively as possible.
- Employees are strictly prohibited from using COMPANY provided IT resources to view, listen to or communicate offensive, defamatory or disruptive content. Such content includes, but is not limited to, material of a sexual or sexually suggestive nature, racial, ethnic or gender-specific slurs, or any other visual / audio / verbal content that offends or is intended to offend someone because of his or her age, sex, religion, disability, etc.

Use of IT resources:

- Users must use COMPANY IT resources only for business activities and in support of the COMPANY business.
- Users must not install, modify or delete any IT or Security applications installed on their systems.
- Users are not allowed to stop any operating system services on desktops, laptops, IT devices provided.
- Users are required to use COMPANY applications and services in a responsible manner:
  - ✓ Email id for employees will be created based on business requirements. Request for email-id will be raised through the Head of Department and forwarded to HR.
  - ✓ Use of email application should be for official purposes only and shall not be used for sending spam, forwards, pictures, etc. especially with defamatory, offensive, racist, religious, sexist content.
  - ✓ Users should take due care to ensure the email is being sent to appropriate users.

	Name	Designation	Signature
Prepared By	B Venkata Rajeev	VP – HR	
Approved By	Gowrinath Atluri	CEO	

- ✓ Users should use classification labels in email subject in case of confidential information transfer.
- ✓ Users should not encrypt or password protect any email, files without authorization.
- ✓ Users should use COMPANY applications in a manner such that data security and confidentiality is not violated.
- ✓ Users should not display classified contents, share access, share printouts, and media with unauthorized people.

- Users should use Internet access for business-related activities, i.e., to communicate with customers and suppliers, to research relevant topics and obtain useful business information.
- Users with Internet access are expected to conduct themselves honestly and appropriately on the Internet, and respect the copyrights, software licensing rules, intellectual property rights, and privacy.
- Users should not use Company IT assets, network or resources to browse restricted or unethical or illegal websites such as porn, gambling, and any other category which are not allowed by IT or company rules.
- Download of content from Internet like text, images which contain material of pornographic, racist or extreme political nature, or which incites violence, hatred or any illegal activity is prohibited.
- Internet should not be used to transmit confidential, political, obscene, threatening, or harassing materials.
- Access to public email facility such as yahoo, Gmail shall be restricted. Exceptions will be made with the approval of CEO/ Director.
- Access to social networking sites such as Facebook, Twitter, etc. is not permitted.
- By default, all USB ports for the desktops/Laptops are disabled. For USB Port enabling, a request has to be raised with the IT Help Desk with prior approval from the Business unit head stating the reason for such access. The request is then assessed and approved by the IT head

Responsibilities

- The users should ensure safety and security of the IT resources allocated; this includes

Laptops, desktops, removable media, etc.

- Personal Laptops or any other device should not be brought to the office and should not be used for business purposes.
- Users are required to safeguard their data, personal information, passwords and authorization codes, and confidential data.
- Users must not share User IDs and password with anyone. All employees shall have a unique logon ID for access to network resources. The creation, modification and disabling of the ID is carried out on requisition and approval from appropriate Business Head / Functional Head in consultation with the Head IT. Unique user IDs are allotted to ensure appropriate accountability and responsibility of user activity.
- Users are responsible for any damage/theft to the IT assets while in their possession.

Illegal Copying

- Users are restrained from illegally copying material protected under copyright law or make that material available to others for copying. Employees are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material one may wish to download or copy. Employees are urged not to agree to a license or download request for any material for which a registration fee is charged, without first obtaining the express written permission of the Company.

Communication of Trade Secrets

- Unless expressly authorized to do so, user is prohibited from sending, transmitting, or otherwise distributing proprietary information, data, trade secrets and other confidential information belonging to company. Unauthorized dissemination of such material may result in severe disciplinary action as well as substantial civil and criminal penalties.

Virus detection

- Files obtained from sources outside the Company, including disks brought from home, files downloaded from the Internet, newsgroups, bulletin boards, or other online services, files attached to e-mail, and files provided by customers or vendors, may contain dangerous computer viruses that may inflict damage the Company's computer network. Users should never download files from the Internet, accept e-mail attachments from outsiders, or use disks from non-Company sources, without first scanning the material with company-

approved virus checking software. If it is suspected that a virus has been introduced into the company's network, employee should bring the same to the notice of the System Administrator immediately.

Privacy and monitoring

- COMPANY may restrict any user's usage of the computing and networking facilities; to copy, remove, or otherwise alter any information or system that may undermine the authorized use of the computing and networking facilities; and to do so with or without notice to the user in order to protect the integrity of COMPANY's computing and networking facilities against unauthorized or improper use, and to protect authorized users from the effects of unauthorized or improper usage.
- COMPANY, through authorized individuals, reserves the right to periodically check and monitor the computing and networking facilities, and reserves any other rights necessary to protect them.

COMPANY reserves the right to take emergency action to safeguard the integrity and security of the computing and networking facilities.

Violations

- The IT Team may initiate action against any person using the computing and networking facilities if found in violation of this policy. The violation also includes: causing physical damage, in possession of unauthorized information, causing destruction of information, causing interruption of IT services, Gaining or attempting to gain unauthorized access to IT assets / data / restricted areas and inappropriate use of the IT Resources

Disciplinary actions

- Violation of these directives may lead to legal and/or disciplinary action up to and including termination of employment. The actions may include:
  - ✓ Suspension
  - ✓ Remarks in personal file
  - ✓ Dismissal
  - ✓ Criminal or Civil action
- Any act of disciplinary actions shall precede with an investigation by the HR, IT Head, and concerned Business / Functional head based on which the course of the disciplinary action

shall be decided.

The Management reserves the right to amend the policy from time to time in line with business requirements.