IT Policy

Information Technology Policy and Procedure Manual

For the Employees of:

NIELIT Kolkata, under MeitY, Government of India

July 2020

National Institute of Electronics & Information Technology (NIELIT) Kolkata

An Autonomous Scientific Society of Ministry of Electronics & Information Technology, Govt. of India

Formerly DOEACC Society Kolkata Centre Since 2003

(Prior to that Regional Computer Centre, Calcutta)

Jadavpur University Campus

Kolkata – 700 032

Telephone: (033) 2414-6081/6054 Fax: (033) 2414-6549

E-mail: dir-kolkata@nielit.gov.in

Website: www.nielit.gov.in/kolkata

PREFACE

National Institute of Electronics & Information Technology (NIELIT), Kolkata IT Policy and Procedure Manual provides the policies and procedures for selection and use of IT within the organization which must be followed by all employees associated with the organization. It also provides guidelines that NIELIT, Kolkata will use to administer these policies, with the correct procedure to follow.

NIELIT, Kolkata will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures.

Any suggestions, recommendations or feedback on the policies and procedures specified in this manual are welcome.

These policies and procedures apply to all employees.

Table of Content

1. About Us

NIELIT (erstwhile DOEACC Society) is an Autonomous Scientific Society under the administrative control of MeitY (Ministry of Electronics and Information Technology), Govt. of India. It was set up to carry out Human resource Development and related activities in the area of Information, Electronics & Communication Technologies (IECT). The Society, has its presence at 40 locations with its head quarters at New Delhi.

The Society is engaged in carrying out Education & Training Programs - both in the Formal & Non- Formal sectors in the area of IECT. Its mandate includes development of Industry oriented quality education and training programs in the state–of-the-art areas, to establish standards and to be the country's premier institution for Examination and Certification in the field of IECT. It is also a National Examination Body, which accredits institutes/organizations for conducting courses in the non-formal sector education in the field of IT and related areas.

NIELIT Centres are conducting long-term courses at Post-Graduate level (M.Tech) in Electronics Design & Technology, Embedded Systems etc. which are not normally offered by Universities/Institutions in the formal sector. Other long term courses conducted by the Centers are Diploma Level courses in Electronics Production & Maintenance, Electronic Engineering, Computer Science & Engineering, Masters in Computer Application, and Bachelor in Computer Applications etc., which are affiliated to respective State Universities/Technical Boards. As for non-formal Sector, the NIELIT Centres are conducting various long term courses viz. NIELIT 'O', 'A', 'B' & 'C' level Courses, Computer Hardware & Maintenance O/A Level and O/A/B level courses in Bio-informatics, Entrepreneurship development, etc. depending upon the demand in respective region. NIELIT also offers Course on Computer Concepts (CCC), Basic Computer Course (BCC), Awareness Computer Course (ACC), which are basically IT Literacy Level Courses for anybody and everybody.

The NIELIT Centres are also imparting training in Short Term Courses in the areas of Information Technology, Electronics Design & Technology, Manufacturing Technology, Maintenance Engineering, ITES-BPO etc. Besides the training activities, NIELIT Centres are offering consultancy services and undertaking software development projects in addition to Govt. sponsored projects in the area of Education & Training, R& D, etc.

Vision

To be the leader in development of industry oriented quality education and training in the state of the art areas, establish standards and be the country's premier institution for examination and certification in the field of Information, Electronics and Communications Technology (IECT)

Objective

- To generate quality manpower and develop skilled professionals in the area of Information, Electronics & Communications Technology (IECT) and allied fields, by providing world class education & training and accreditation services.
- To provide continuing support to learners and trainers through active design & development of innovative curricula and content aligned with the dynamically changing IECT scenario as and when required.
- To establish a globally recognized quality system of examination and certification and provide a fair assessment of the competency of students.
- To continue to implement various NIELIT Schemes in the Non- Formal Sector in the IECT area.
- To establish standards in the area of IECT and to develop market oriented courses in the emerging areas as per the need.

- To impart continuing education for up-gradation of knowledge and skills of Industry professionals & academicians considering high obsolescence in the area of IECT.
- To provide entrepreneurship development program in the area of IECT.
- To develop and promote the culture of market to encourage and nurture industry oriented design and development.
- To provide Consultancy and Services to Government and non-Government Organizations in IECT

Activities of the NIELIT (HQ) and its Centres

Core activities of the Society - Education & Training in the area of Information, Electronics and Communication Technology (IECT) are different from other educational programs of similar nature, in scope and quality, in the following aspects:

- Flexible programs with consistent and timely updating of Course Curricula to conform to industry needs, so that the students graduating from the Society should not only find employment but also be sought after by the Industry,
- Industry participation in the formulation and running of programs, particularly for imparting hands-on-experience.
- Latest Technology is used in all operations of the Society.
- Regular feedback from customers i.e. students and Industry

The above IT Education & Training Programs are categorized as follows:

- IT Education & Training for fresh students;
- Continuing Education (Refresher training/up-gradation) for working professionals through Short-Term/Long-Term Courses; Training of Trainers at various levels; and New courses in emerging areas of IECT

The Society is also engaged in Data Processing, Software Development and Consultancy projects in addition to Education & Training Programs.

2. Equipment Usage Policy

2.1 Objective

The Equipment Usage policy informs employees and officers about equipment purchase, organizational and project level inventory management, rules for allocating & transferring equipment to employees, departments or projects and best practices for all equipment usage and maintenance.

2.2 Equipment Purchase

1) The following equipment is purchased by the organization and provided to individual employees, departments or projects for their official use. The list can be modified as and when required.

   a) Personal Computing Devices (Desktop, Laptop)
   b) Computer Peripherals (Printer, Scanner, Photocopier, Keyboard, Mouse, Web Camera, Speaker, Modem etc.)
   c) Networking Equipment & Supplies (Router, Switch, Antenna, Wiring, etc.)
   d) Biometric Devices

2) The Procurement Dept. procedures & guidelines need to be followed to purchase new equipment for official purposes. All approved equipment will be purchased through the Procurement Dept., unless informed/permitted otherwise.

3) The Procurement Dept. will maintain a small inventory of standard PCs, software and equipment required frequently to minimize delay in fulfilling critical orders.

2.3 Equipment Usage, Maintenance and Security

1) It is the responsibility of all employees to ensure careful, safe and judicious use of the equipment & other assets allocated to and/or being used by them.

2) Proper guidelines or safety information must be obtained from designated staff in the IT Dept. before operating any equipment for the first time.

3) Any observed malfunction, error, fault or problem while operating any equipment owned by the organization or assigned to you must be immediately informed to the designated staff in IT Dept.

4) Any repeated occurrences of improper or careless use, wastage of supplies or any such offense compromising the safety or health of the equipment and people using them will be subject to disciplinary action.

5) If your assigned computing device is malfunctioning or underperforming and needs to be replaced or repaired, then written approval from your Reporting Officer is required for the same. The malfunctioning device needs to be submitted to the IT Dept. for checking, maintenance or repair. The IT Dept. staff person will give a time estimate for repair/maintenance.

6) The Reporting Officer can be informed about excessive delay or dissatisfaction about the repair or maintenance performed by the IT Dept. The issue will then be resolved by the Reporting Officer in consultation with the IT Dept. Head. The Management Committee can be consulted in terms of serious disputes or unresolved issues.

2.4 Phone Usage Policy

1) Landline phone systems are installed in the organization's offices to communicate internally with other employees and make external calls.

2) The landline phones should be strictly used to conduct official work only. As far as possible, no personal calls should be made using landline phones owned by the organization.

3) Long distance calls should be made after careful consideration since they incur significant costs to the organization.

4) The Admin. Dept. is responsible for maintaining telephone connections in offices. For any problems related to telephones, they should be contacted.

5) Employees should remember to follow telephone etiquette and be courteous while representing themselves and the organization using the organization's phone services.

3. Personal Computer (PC) Standards

3.1 Objective

The main aim of this policy is to maintain standard configurations of PC hardware and software purchased by the organization and provided to employees for official work. The hardware standards will help maintain optimum work productivity, computer health & security and provide timely and effective support in troubleshooting PC problems. The software standards will ensure better system administration, effective tracking of software licenses and efficient technical support.

3.2 General Guidelines

1) It is the responsibility of the IT Dept. to establish and maintain standard configurations of hardware and software for PCs owned by the organization. The standard, can however, be modified at any point in time as required by the IT Dept. Head in consultation with the Management Committee.

2) Multiple configurations are maintained as per the different requirements of various departments and projects in the organization, in consultation with the Dept./Project Head.

3) Only in exceptional cases, when none of the standard configurations satisfy the work requirements, an employee may request a non-standard PC configuration. Valid reasons need to be provided for the request and written approval of the Reporting Officer(s) is required for the same.

3.3 Network Access

1) All PCs being used in the organization are enabled to connect to the organization's Local Area Network as well as the Internet.

2) Network security is enabled in all PCs through Firewall with inbuilt securities.

3) Employees are expected to undertake appropriate security measures as enlisted in the IT Policy.

3.4 Data Backup Procedure

Data Backup is setup during installation of Operating System in a PC. As an additional security measure, it is advised that employees keep important official data in some external storage device also.

4. Internet Usage Policy

4.1 Objective

The Internet Usage Policy provides guidelines for acceptable use of the organization's Internet network so as to devote Internet usage to enhance work productivity and efficiency and ensure safety and security of the Internet network, organizational data and the employees.

4.2 General Guidelines

1) Internet is a resource and therefore shall be used only for office work.

2) The organization reserves the right to monitor, examine, block or delete any/all incoming or outgoing internet connections on the organization's network.

3) The organization has systems in place to monitor and record all Internet usage on the organization's network including each website visit, and each email sent or received. The Management Committee can choose to analyze Internet usage and publicize the data at any time to assure Internet usage is as per the IT Policy.

4) The organization has installed an Internet Firewall to assure safety and security of the organizational network. Any employee who attempts to disable, defeat or circumvent the Firewall will be subject to strict disciplinary action.

5) An employee can also get a local static IP address for Internet and intranet use. All employees will be responsible for the Internet usage through this local static IP.

6) All employees may be provided with a Username and Password to login to the wi-fi Internet in the office and to monitor their individual usage. Wi-fi Username and password allotted to an employee will be deleted upon resignation / termination/retirement from the organization.

7) A visitor or guest user who wants to use the office Internet will be given a local static IP address for Internet and intranet use. He may also be given a Guest Username and Password for connection to the wi-fi Internet.

8) The employee will be held responsible for all the network traffic generated by "his computer". The employee should understand that network capacity is a limited, shared resource. Physically tampering with network connections/equipments, sending disruptive signals, or making EXCESSIVE USE of network resources is strictly prohibited. Repeated offenses of this type could result in permanent disconnection of network services. The employee should not share the network connection beyond his own use and should not act as a forwarder/ masquerader for anyone else. The employee will be held responsible for the content stored in the designated workspace allotted to him (examples: file storage area, web pages, stored/archived emails, on Servers or Department machines).

9) The employee should not attempt to deceive others about his identity in electronic communications or network traffic. He also should not use IT resources to threaten, intimidate, or harass others.

10) The employee should not intrude on privacy of anyone. In particular he should not try to access

computers (hacking), accounts, files, or information belonging to others without their knowledge and explicit consent.

11) Employee should understand that he should not take any steps that endanger the security of the NIELIT Kolkata network. Specifically, he should not attempt to bypass firewalls and access rules in place.

12) Employee should not use the IT infrastructure to engage in any form of illegal file sharing (examples: copyrighted material, obscene material).

13) Electronic resources (such as e-journals, e-books, databases, etc.) are for academic use only and these resources can be searched, browsed, and material may be downloaded and printed as single copies of articles. Downloading or printing of a complete book or an entire issue or a volume of one or more journals (called systematic downloading) is strictly prohibited. Use of robots, spiders or intelligent agents to access, search and/or systematically download from the e-resources is also prohibited. Any violation of this policy will result in penal action as per the rules and regulations of the Institute.

14) Employee should not host or broadcast information that might harm others or may be otherwise considered objectionable or illegal as per Indian law.

5. Software Usage Policy

5.1 Objective

The Software Usage Policy is defined to provide guidelines for appropriate installation, usage and maintenance of software products installed in organization owned computers.

5.2 General Guidelines

1) Third-party software (free as well as purchased) required for day-to-day work will be pre- installed onto all company systems before handing them over to employees. A designated person in the IT Dept. can be contacted to add to/delete from the list of pre-installed software on organizational computers.

2) No other third-party software – free or licensed can be installed onto a computer system owned or provided to an employee by the organization, without prior approval of the IT Dept.

3) To request installation of software onto a personal computing device, an employee needs to send a written request via the IT Support Email.

4) Any software developed & copyrighted by the organization belongs to the organization. Any unauthorized use, storage, duplication or distribution of such software is illegal and subject to strict disciplinary action.

5.3 Compliance

1) No employee is allowed to install pirated software on official computing systems.

2) Software purchased by the organization or installed on organizational computer systems must be used within the terms of its license agreement.

3) Any duplication, illegal reproduction or unauthorized use and distribution of licensed software within or outside the organization is strictly prohibited. Any such act will be subject to strict disciplinary action.

4) The Procurement Dept. procedures & guidelines need to be followed to purchase new software (commercial or shareware) for official purposes. All approved software will be purchased through the Procurement Dept., unless informed/permitted otherwise.

5) Any employee who notices misuse or improper use of software within the organization must inform his/her Reporting Officer(s).

5.4 Software Registration

1) Software licensed or purchased by the organization must be registered in the name of the organization with the Job Role or Department in which it will be used and not in the name of an individual.

2) After proper registration, the software may be installed as per the Software Usage Policy of the organization. A copy of all license agreements must be maintained by the IT Dept.

3) After installation, all original installation media (CDs, DVDs, etc.) must be safely stored in a designated location by the IT Dept.

5.5 Software Audit

1) The IT Dept. will conduct periodic audit of software installed in all organization owned systems to make sure all compliances are being met.

2) Prior notice may or may not be provided by the IT Dept. before conducting the Software Audit.

3) During this audit, the IT Dept. will also make sure the antivirus is updated, the system is scanned and cleaned and the computer is free of garbage data, viruses, worms or other harmful programmatic codes.

4) The full cooperation of all employees is required during such audits.