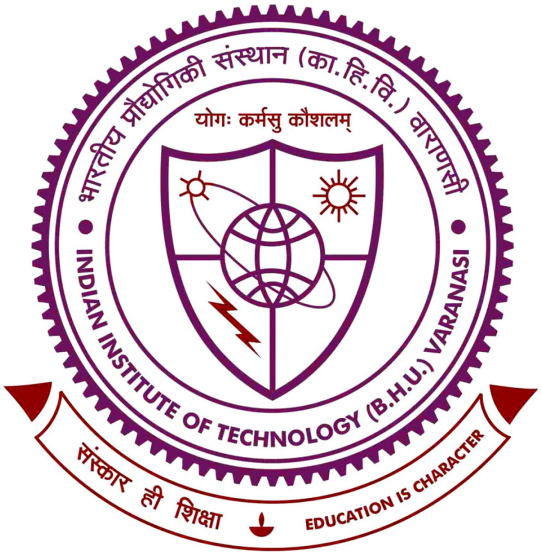
Computer Assets (CA)

and

Information Technology (IT)

(Usage) Policy

CAIT POLICY



INDIAN INSTITUTE OF TECHNOLOGY

(BANARAS HINDU UNIVERSITY),

VARANASI (U.P.) – 221 005

INDIAN INSTITUTE OF TECHNOLOGY (B.H.U.)

DOCUMENT CONTROL SHEET

1.	Security Classification	Unrestricted			
2.	Distribution	All the students, staff, faculty members of IIT (BHU) and others using computer, information and communication technologies, within the Institute's network (including VPNs on global/ local networks)			
3.	Document Version	Issue No.	01	Revision & Date	NA
4.	Document Type	Policy Document			
5.	Document Control Number	IITBHU/CISO/ 2015-16/ 01 Dated April 24, 2015			
6.	Title	Computer Assets and Information Technology (usage) Policy (CAIT Policy), IIT (BHU)			
7.	Compiled by	Dr. N. S. Rajput			
8.	Affiliation towards compilation	Chief Information Security Officer, IIT (BHU)			
9.	Scrutiny Mechanism	Compiled by Dr. N. S. Rajput	Reviewed by Prof. S. Rawat	Approved by Prof. R. Sangal	
10.	Date of Initiation	April 24, 2015			
11.	Date of Issue/ Publication	June 16, 2015			
15.	Abstract/ Keywords	IIT(BHU), IT Policy, National Cyber Security Policy, Cert-in, Information Technology Act, CISO, CAIT Policy			
16.	References, Courtesy and Credits	IT Policy documents of: IIT-Bombay, ETH-Zurich, MIT and Stanford University and Student's team, EC Department, IIT(BHU): Naimesh Maddula, Ayush Singh and Nairit Mondal			

Index

Computer Assets and Information Technology (usage) Policy
IIT (BHU)

This policy is the guideline for appropriate use of all information technology enabled resources (but not limited to) such as computers, networks, and the information contained therein.

Authority:

Approved by the competent authority of IIT BHU.

Applicability:

This policy is applicable to all the students, faculty members, staff of IIT (BHU) and all others who use institutional Information Technology (IT) resources (i.e. all the computers, communication nodes, information and communication technologies (ICT) etc.), within the Institute's network and access, transmit or store Institutional and/ or personal information.

All such aforesaid users SHALL be required to sign an undertaking placed as Annexure – I, at the end of this document.

Policy Statement:

IT resources of the Institute should be used to augment various objectives of teaching, learning and research. It is the responsibility of the Users of IIT (BHU) network and computer resources ("users") to appropriately use and protect institutional IT resources and to respect the rights of others. This policy is a guideline for safer and legitimate use of such IT resources.

1. Definitions

Terminology as used in this policy:

1.1. "Information Technology (IT) Resources" : This includes all the devices and technologies provided by the Institute, which access, process, store or transmit Institute's or an individual's personal information.

1.2. "Information" includes both Institute's and an individual's personal information, both in public or personal domain.

1.3. "Individually owned resources" are IT resources that are purchased and owned by individuals and are being used within Institutional prerogatives.

2. Policies

2.1. General Policy

The Institute recommends its Users to safeguard

(i) the integrity of IT resources,

(ii) the privacy of electronic information, and

(iii) their own online identity from use by another individual.

User should not attempt to retrieve or gain unauthorized access to any other user's accounts and their IT resources. Users should safeguard the rights and privileges of owners and publishers over all copyrighted materials, licenses and on other information resources, no matter whether claimed or not.

2.2. Access to IT Resources

The Institute prohibits its users from gaining or enabling unauthorized access to forbidden IT resource on the Institute network. Any such attempt will not only be the violation of Institute Policy but may also violate national and international cyber laws, provisions under The Information Technology Act of India and infringe the principals of National Cyber Security Policy, and subject the user to both civil and criminal liability.

However, the Institute reserves all the rights to access and analyze the IT resource and Information for any legal and/ or institutionally provisioned operation, on its own or through its affiliates.

2.2.1. Non-transferable Identities

All user identities on the Institute network are non-transferable and shall not be shared or used by any other user. Any such known or unknown usage shall constitute violation of the Institute policy.

2.2.2. Proprietary nature of information

All the information belonging to other users (such as data, programs or any other digital material, passwords etc.) shall remain proprietary in nature and without obtaining specific permissions form respective users, other users shall not use or possess or share any such information in its original or modified form.

2.3. **Legitimate Use of IT resources**

The users of IT infrastructure of the Institute are also by default governed by the prevailing laws of the land. Further, current policy document broadly indicates Institute's commitment towards observing such security mandates and legal bindings. The 'users' are therefore also advised to be aware and remain compliant to various legal obligations, licenses, contracts and prevailing Information Technology Act of India, National Cyber Security Policy, etc.

2.3.1. **Prohibited Use**

The Institute prohibits its users from sending, viewing or downloading fraudulent, harassing, obscene (i.e., pornographic), threatening, or other messages or material that are a violation of applicable law or Institute policy. Therefore, user's inhibitive discretion is solicited where category of certain content could be doubtful e.g. when such content is received through e-Mail etc.

As a generalized policy, any contribution towards the destruction or distortion of congenial academic or work environment is prohibited.

2.3.2. **Caution regarding Copyrights and Licenses**

Users must not violate various IPR and copyright law(s), and licensing policies as associated with copyrighted materials and software. Any unlawful file-sharing, use of any form of illegal or pirated or un-licensed software, on the Institute's IT resources (including individually owned IT resource being used under Institutional IT privileges) is strictly prohibited and any such act shall constitute a violation of the Institute policy.

Institute also recommends to its students, faculty and office staff, to use Open Source Operating Systems (OS) and Processing Software (PS) such as **Ubuntu/ CentOS or other** and **Libre Office/ OpenOffice/ WPS Office,** respectively. Further, users of the computers sponsored directly or indirectly by IIT (BHU) should migrate on the recommended OS & PS as their primary software and should generate expertise on it. In case of technical limitation in such adaptation, relaxation may be requested from competent authority on valid grounds.

2.3.3. **Terms of Use of Social Media**

By agreeing to abide by the terms of use of various online media forums, the users are expected to adhere with the norms as prescribed by respective social networking websites, mailing lists, chat rooms, blogs, etc.

2.3.4. **Personal Use**

The Institute's IT resources should not be used for activities that are un-connected with Institute's prerogatives towards research and academic functions, except when there is urgency to check personal e-Mails, bank and other social accounts, news etc.

2.3.5. **Commercial Use**

The Institute prohibits use of its IT resources for any commercial purpose except when permitted by appropriate authority. Further, when any such use is permitted, it should be properly related to Institute activities, and after taking into account all additional liabilities, as may accrue by reason of such activity.

2.3.6. **Access to and use of IT Resource/ Data**

The Institute may generate huge data containing variety of information. For conducting any study or analysis on such IT resource, prior approval from competent authority MUST be obtained and users must abide by the terms and conditions of grant of such approvals, applicable privacy and other policies.

2.4. **Use of individually Owned IT Resources**

The Institute does not require or recommend use of individually owned IT resources to conduct institutional tasks. However, individual units may allow its users to use such IT resource within the unit only and any such user may choose to use his/her own IT resources and abide by respective terms and conditions.

Further, any such use must comply with the Institute policies esp. CAIT Policy, IIT (BHU) and other requirements for which such use has been permitted.

2.5. **Confidentiality, Integrity and Availability (CIA) of IT Resources**

Users must respect and maintain adequate level of confidentiality, integrity and availability of information and IT resources.

2.5.1. **Confidentially**

Unless a user has proper authorization, no user should attempt to gain access to information and disclose the same to self or other unauthorized users. The broader concept of data privacy must be honoured by each user.

2.5.2. **Integrity**

No user should attempt to vandalize, damage or change any data inappropriately, whether by accident or deliberately. The basic notion of trustworthiness of information resources must be preserved by all of its users. Any interference, disruption or encroachment in the Institute's IT resources shall be a clear violation of the Institute policy.

2.5.3. **Availability**

No user should attempt to affect the availability of IT resource, whether accidently or deliberately.

2.6. Extension of Computer Assets and IT (Usage) Policy

As long as individual departments, schools, individual units etc. can retain consistency in compliance of the IT (Usage) Policy (CAITP), IIT (BHU), they may further define and implement additional "conditions of use" for IT resources under their control. It will be the responsibility of the Units to publicize and enforce such conditions of use. In cases where use of external networks is involved, suitable policies can be practiced in compliance with the broad prerogatives of (Usage) Policy of the Institute.

2.7. Access of Information to Legal and Institutional Bodies

As a part of certain investigation procedures, the Institute may be required to provide its IT information, resource and/ or records, in parts or full, to third parties. Also, for proper monitoring and optimal utilization of institutional IT resources, the Institute may review, analyze and audit its information records, without any prior notice to its Users. Further, the Institute may also seek services from third-party service providers. Accordingly, the users can only have reasonable expectation of privacy on the Institute's IT resources.

3. IT Resource Management

Management and operation of IT resource is the responsibility of concerned head of respective subdivision to which that IT resource belongs. In IIT (BHU), it could be the Dean, Head of Department, Coordinator of School, Principal Investigator, Coordinator of certain facility or any other competent authority with whom such IT resource has been associated. Compliance of the Institute's Computer Assets and IT (usage) Policy shall be the sole responsibility of the aforesaid officials for the IT resources of their concern. For convenience, aforesaid officials may designate another person to manage and operate respective IT resource (designated as "system administrator") but responsibility for policy compliance on respective IT resources shall still remain with the concerned official only.

The system administrator will manage and operate IT resources as per the policies of the Institute and of the concerned sub-division. He/ she will also refer to the Information Security Office, any matter, which is beyond maintenance and operation of such IT resource.

3.1. Responsibilities of the System Administrator

The system administrator should:

- Educate users regarding various nuances of Institute's Computer Assets and IT (usage) policy and other prevailing national and international policies and developments
- Help users implement and comply with the Institute policies and help users execute and maintain faithfully all licenses on their IT resource
- Secure and protect IT resources by taking befitting actions
- Prevent and protect IT resources from damage or theft
- Coordinate with the Chief Information Security Officer to seek recommendations and guidelines for implementation, and to find and correct problems associated with the systems and network under their control

3.2. Loss of Use Privileges and Suspension of User Access

Consequent upon any inappropriate usage (abuse) of IT resources or in cases of repeated offences of abuse, it will be the sole prerogative of the system administrator to temporarily suspend or permanently terminate any user's access to IT resources, with (preferred) or without (if required urgently) any prior warning to the user. However, after taking such a preventive measure, such cases shall be referred to competent authority and with information to the concerned user.

4. Disabling IT Resource/ User's network connectivity

4.1. Network Infrastructure Liability

The Institute holds responsibility of managing and protecting the IIT (BHU) network(s) against electronic forms of attack or abuse. It is the sole prerogative of the Institute to terminate network connections to computers within its domain due to suspected or actual abuse of the network and/or its components.

4.2. Termination of Connection to an Offending Computer

The network connection to an offending computer may be terminated by disabling the port of that particular switch which connects the offending computer to communicate with the Internet and further traffic to and from that computer will be stopped. Local applications on the computer, however, will remain unaffected after such termination.

4.3. Terminating a Connection with warning

Depending upon the urgency of taking preventing action(s), concerned Users will be informed regarding their machines which are causing disturbances and an action from the user end will be solicited within a specified time-frame beyond which action can be taken from the System Administrator's side.

5. Reporting and Investigations of Policy Violations

5.1. Reporting of Policy Violations

It is the duty of users to report policy violation(s) before appropriate authority or a concerned official, especially when issues are related with

accounts, system security, or when they have information about unlawful or suspected abuse of IT resources, through e-Mail or in person, during normal office hours.

5.2. Inspection of IT Resource and Information Records

In the interest of better safety of user(s) or the user community, appropriate policy compliance or due to legal proceeding, all or part of IT resources may be monitored and/ or analyzed or audited with or without any prior notice to any or all the users, by the Institute or through third-party service providers. Only the Director, IIT (BHU) (or designate) may authorize this type of exhaustive inspection and monitoring.

5.3. Teamwork and Cooperation

The Institute solicits wholehearted cooperation and sincere support from its users of IT resource during any investigation of policy abuse and/ or cyber crime. Instances of non-cooperation from any user shall constitute the grounds for suspension or cancellation of access to IT resources or other disciplinary actions.

6. Non-compliance of CAIT Policy and Consequent Abuse

Non-compliance of the CAIT Policy and consequent abuse of IT resources may attract appropriate disciplinary action up to and including discharge, dismissal, expulsion, and/or legal action. Violation of this policy may also indicate that a user may also have violated the legal prerogatives as permitted under prevailing cyber laws and acts. If established, such action may also lead to severe civil or criminal proceedings as per the applicable laws and provisions.

The Chief Information Security Officer (CISO) will refer such violations to the Director, IIT (BHU) for seeking further necessary directions.

CAUTION: Various laws as applicable in real world may also be applicable in cyberspace (including IIT (BHU)'s Network). Users of IT resources are ***not*** exempted from existing laws about libel, harassment, privacy, copyright, licenses, stealing, threats, etc. Taking precautions and preventive measures while using cyber space and IT resources may be the best saviour. Any abuse of IT resources may lead to severe consequences and legal proceedings.

ANNEXURE - I

Computer Assets and Information Technology (usage) Policy
IIT (BHU)

Mandatory Undertaking

By signing-up this declaration (Annexure – I), the signatory user will hereby adopt and enact the Institute's "Computer Assets and Information Technology (usage) Policy" along with the following explicit Undertaking.

1. **[My Computer]** I understand that the term "My Computer" binds me with all the IT resource for which I am responsible. I shall be responsible for all of my usage and activities on Institute's IT resource. I shall bear full responsibility for all the content on my personally owned IT resource (computer(s), mobile, tabs etc.) which I operate within IT resource prerogatives of the Institute. Also, I will own similar responsibility, on all the IT resources as allotted to me by the Institute, including its stored and shared content (for example: file storage area, web pages, stored/ archived emails, compute and storage nodes, NAS and SAN etc.).

2. **[My Software]** I will be responsible for all the Software as installed, copied and operated on 'My Computer'. I will also NOT infringe with the copyright and licensing policy of each software as present in my computer. I will also NOT indulge in any unauthorized duplication, distribution or use of computer software than the license allows, or install software onto multiple computers or a server which has been licensed for one computer only. I will also NOT aid to piracy by providing unauthorized access to software by way of providing serial numbers used to register software. I also understand that the Institute is committed to run legally licensed software, and that the institute does not support software copyright infringement in any form.

3. **[My Network]** I will hold responsibility for all the network traffic generated from "my computer". I will not attempt to physically tamper or access remotely any network connection(s)/ equipment(s), send disruptive signals, or over use of network resources. I understand that repeated abuse as indicated in this policy document could result in permanent termination of my IT resource access privileges disconnection of network

services. I shall not act as a forwarder on/ masquerade any network connection for anyone else and would access the IT resources for my own individual use.

4. **[My Communication]** I shall also not use Institute IT resources to threaten, intimidate, or harass others or to send wasteful broadcasts and malicious mail broadcasts. I shall also not attempt to deceive and spoof my identity while using IT resources.

5. **[Principles of Use]** I understand that the institutional IT resource is for academic and research purpose only. I shall not use it for any other purpose including any commercial or data hosting services for other people or groups, both on local and global network. I shall also not host shared files or information that might be otherwise considered objectionable or illegal under prevailing IT Act and other Cyber Laws.

6. **[Privacy Rights]** I shall respect privacy rights of all users. By any means, I shall not indulge into or attempt to gain unauthorized access of any IT resource belonging to other user(s) and without their knowledge and explicit consent. This includes any attempt to hack other user's computers, accounts, files, data, programs or any other information resource. I also understand that 'forgery' or other misrepresentation of one's identity via electronic or any other form of communication is a 'Fundamental Standard violation' and may attract severe legal actions.

7. **[IT Resource Monitoring]** I understand that the all IT resources of Institute are subject to monitoring as per the Institute policy. The monitoring may include aggregate bandwidth usage, monitoring of traffic content etc. in response to compliance of any national or institutional policy or due to request from law enforcement agency. I understand that the Institute has authority to perform network vulnerability and port scans on my systems (without any prior notice), as and when needed, to ensure integrity and optimal utilization of IT resources.

8. **[Protection from Viruses]** I understand that viruses may severely degrade the performance of IT resources and it is my responsibility to keep my computer updated, by using available virus detection software and operating system updates.

9. **[Prohibition in File Sharing]** I understand that sharing and hosting of any copyrighted or obscene material is strictly prohibited. I also understand that the electronic resources under IT resources such as e-journals, e-books, databases etc. are for personal academic use only. Bulk download or printing of complete book or

downloading complete issue of any journal is strictly prohibited and may infringe with the policy of the library or terms of use of the publishers.

10. **[Security Compliance]** I understand that any attempt to endanger the security and stability of the IT resource is strictly prohibited. I undertake that by any means, deliberate or unknowingly, I shall not attempt to bypass firewalls and access rules as configured. I will not attempt to set-up any unauthorized server(s) and client(s) of any kind (e.g. vpn, proxy, mail, web or hub etc.) both on local or global network by misusing institutional IT resource. I understand that any such careless act may lead to suspension or permanent loss of IT resources access privileges along with other suitable disciplinary action(s) etc.

11. **[Consequences of Non-compliance]** I understand that any abuse to and non-compliance of Computer Assets and IT (Usage) (CAIT) Policy and any other act that constitutes a violation of Institutional Rules & Regulations could result in administrative or disciplinary procedures.

I hereby undertake to abide by the CAIT Policy and other rules and regulations of the Institute and adopt and enact this with immediate effect.

Signature of the User……

Name & Affiliation of the User……

……

……

Place……

Date……