Dibrugarh University IT Policy

Version - 1.0

1. Policy Statement

The objective of this policy is to bring a systematic approach to the overall Information Technology (IT) resources used by the administration, faculty, and students at Dibrugarh University. The policy looks at acquisition, maintenance and disposal of the IT resources along with various user guidelines and responsibilities.

2. Need for the IT Policy

Dibrugarh University has sizeable IT resources for its operational needs. With increasing use of the IT resources for various works by the administration, faculty, and students, it is felt that proper policies and guidelines should be in place for the proper use of the IT resources and prevent its misuse.

3. Definitions

3.1 Authorized Users: Authorized users are people who have been provided User Id and Password. They can log in and update their profiles/use the systems.

3.2 Computer Hardware: In the context of this policy, computer hardware is defined as desktop, laptop, notebook, or any variation of computer equipment that the university uses for educational or instructional purposes that can have its operating system and core software imaged. Also included in this definition would be tablets or other smart devices acquired by the University out of its funds for use as specified above.

3.3 Computer Networks: Include any local or wide area communications systems connecting above defined computer systems or hardware.

3.4 Computer Systems: Include any personal computer *(stand-alone or networked)*, workstation, thin clients or server used on this campus or accessible by way of networks at other locations, acquired and possessed by the University.

3.5 Content Contributors: Content Contributors are people inside University who provide materials to be published on the website. They may be officers, employees or teachers of the University who may provide data for the website.

3.6 Cyber Crime: It is a generic term that refers to all criminal activities done using the medium of computers, the Internet, cyber space and the worldwide web.

3.7 Cyber Law: It is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace", i.e. the Internet. It is less of a distinct field of law in the way that property or contract are, as it is an intersection of many legal fields, including intellectual property, privacy, freedom of expression, and jurisdiction. In essence, cyber law is an attempt to apply laws designed for the physical world, to human activity on the Internet. In India, The IT Act, 2000 as amended upto date is known as the Cyber law. It has a separate chapter XI entitled "Offences" in which various cyber-crimes have been declared as penal offences punishable with imprisonment and fine.

3.8 Cyber Security: It is defined under Section (2) (b) of Information Technology (amendment) Act-2008. It means protecting information, equipment, devices computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

3.9 Data Entry Operator: Data Entry operator has limited back end access to the website. He/She can publish official notifications, results, tenders and news & events and upload required files.

3.10 Department Web Administrator: Department Web Administrator is a person who is in charge of the pages of his/her Department/Centre/Branch. Department Web administrators can access the backend, but it is limited to updating the pages of his/her department/centre/section or other pages authorized to him/her.

3.11 E-mail Fraud: Fraud whether financial, banking and social committed with the aid of an email would be called as email fraud.

3.12 E-mail Spoofing: It is an e-mail activity in which the sender addresses and other parts of the e-mail header are altered to appear as though the e-mail originated from a different source. E-mail spoofing is sending an e-mail to another person so that it appears that the e-mail was sent by someone else. A spoof email is one that appears to originate from one source but actually has been sent from another source.

3.13 Hacking: It means unauthorized attempts to bypass the security mechanisms of an information system or network by users. It is the unauthorized access to a computer system, programs, data and network resources.

3.14 Identity Theft: It is a form of fraud or cheating of another person's identity, in which someone pretends to be someone else by assuming that person's identity, typically in order to access resources or obtain credit and other benefits in that person's name. Information Technology (Amendment) Act, 2008, crime of identity theft under Section 66-C, whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person known as identity theft.

3.15 Network Administrator: An individual responsible for maintenance of computer hardware and software systems that make up a computer network including the maintenance and monitoring of active data network or converged infrastructure and related network equipment.

3.16 Pornography: The graphic, sexually explicit depiction of anybody through pictures or through words that is either verbal or pictorial and which represents or describes sexual behaviour that is degrading or abusive to one or more of the participants in such a ways as to endorse the degradation.

3.17 Web Administrator: Web administrator has the full backend access to the system. He/she can edit the webpages. However, he/she cannot change the structure and the content management system of the website

3.18 Web Developers: Web developers are people who have developed the basic structure and content management system of the website. They can change the basic structure of the system.

3.19 Web Users: Web Users are people who browse the website within the "*dibru.ac.in*" domain name. They don't have the backend access of the website.

3.20 Website: The website corresponding to the URL "http://www.dibru.ac.in" is the official website of Dibrugarh University. The "official" home page structure includes the home page, the linked driven pages, and other pages integrated into the home page structure.

4.1 Policy for Hardware & Software Management

Computers and related software and peripherals purchased by the University, will be managed and maintained by the University. Individual users may not install software or physical devices that prevent appropriate University personnel from accessing the equipment or software to conduct management or maintenance functions. The University may install software on university-purchased PCs or personal PCs connected to the internal (authenticated) campus network to do remote management and maintenance of computers and to protect the computers from viruses, malicious software *("malware" and spyware)*,

etc. The Equipment Purchase Committee of the University shall have overall responsibility for the standards of acquisition, maintenance and inventory control of the University standard-compliant hardware and software.

To accommodate varying needs in administration, instruction, and research computing, while avoiding excessive variability in equipment and software, university computing purchases shall be standardized on the operating systems in use (Windows/Linux/Others). Determination of which system to choose shall be dependent upon the defined use. To promote the standardization of equipment and realize economies-of-scale cost savings in the procurement and maintenance of computing equipment, a list of standard hardware configurations (e.g. value, standard, and high performance) will be established and continuously updated that must be used by University faculty and staff, unless a departmental request for deviation from the standard has been duly approved at the appropriate level/authority.

University desktop/laptop computer programs shall be standardized on selected vendor software packages *(i.e., spreadsheet, word processing, antivirus, and antimalware, etc.)*. When required to submit a document as a computer file to another University department or person, the department or person who submits the file is responsible for providing it in the standardized format. A Windows-based application should be used for administrative purposes if a compatible cross-platform version does not exist. As and where possible, the University will promote the use of Open Systems.

All software products purchased with university-controlled funds shall have proof of license on file with the department ordering it. Information shall include product identification, license number, date of purchase, and user. Departments must maintain such records for software installed locally on computers under their control. Records for software installed to run on the central computer system or from network servers must be duly maintained by the concerned authority. Before purchase of new software, it will be found out whether such software has already been purchased and it has still installable licences. If that is the case, the software will not be purchased again.

Concerned authority will be responsible for maintaining standards-compliant software and hardware. Departments purchasing non-standard hardware or software are responsible for its maintenance. Users shall be responsible for maintaining a backup copy of their software products *(license permitting)*, applications, and data files. Desktop/laptop computer and server-based applications developed by a department rather than by the University authority shall be the responsibility of the concerned department.

The University will maintain an inventory of all systems as well as software. It will annually publish an obsolescence schedule, giving at least a one-year's notice as to what software or

hardware will no longer be supported. Once software or hardware reaches that cutoff date, it will be replaced by the University if the software or hardware is their responsibility. If it is not, the University will not be obligated to provide support for it. Software or hardware replaced by the University may not be retained by the department, but must be turned over to the University for disposing. The user is responsible for removing any data from a desktop/laptop computer before it is replaced. Disk drives from replaced desktop/laptop computers will be physically destroyed by the University before they are disposed of.

Desktop/laptop computer and server-based operations critical to the mission of the University shall have a Disaster Recovery Plan. The responsibility for identifying desktop/laptop computer operations critical to the mission of the University and insuring that a Disaster Recovery Plan for that operation exists rests with the University.

The following ways may be used for disposal of obsolete items:

- **Re-deploy**: Computers that are not capable of performing their intended tasks may still be capable of performing other tasks and thus may be used either within their own or another University department/office. Such computers must be re-deployed within the University.
- **Donate**: Obsolete computers and peripherals that are still operational (but no longer of use to the University) may be donated to non-profit organizations, when donating the equipment furthers one or more of the University's exempt purposes (education, research and community service).
- **Sell**: Obsolete computers and peripherals that are still operational (but no longer of use to the University) may be sold at fair market value to individuals, non-profit organizations or for-profit entities through proper tendering process.
- **Recycle**: Computers and peripherals which may be of such age or condition that they cannot be used for their intended purposes should be recycled. All electronic materials should be recycled in accordance with environmental rules and regulations in place.

As for software, a library of all obsolete software will be maintained for possible use in the future out of necessity or emergency.

The process for disposal of obsolete items will be as specified below:

- **Step #1 - Identification**: Those items will be considered obsolete whose technology has got outdated or which have outlived their utility or whose maintenance cost has become untenable.
- **Step #2 - Authorization**: In all cases, the re-deployment, recycling, donation or sale of equipment must be approved in writing by the appropriate authority.

- **Step #3 - Local redeployment**: If the equipment is identified as obsolete but is still operational, the preferred option is to redeploy it for another use within the unit. After meeting the requirements of Step #4, no further actions are needed with this option, and the remainder of this procedure may be ignored. This is the preferred method for the University.
- **Step #4 - Data removal**: (*Note*: Correct removal of files from equipment is an absolutely irreversible process. Proceed with care.) All data removal must be properly authorized in writing by the appropriate authority. When the equipment will not be recycled, the Authority is responsible for ensuring that all files have been removed from the equipment. In addition to hard drives, other electronic media (DVD, CD, diskette, zip drive etc.,) must be physically destroyed to be rendered unreadable.
- **Step #5 - Software License Accounting**: Software that has been licensed under University contracts must be removed from equipment that is being donated or sold outside of the University. If the machine is to be re-deployed within the University such software must be deleted if the licensed software is to be installed on the system replacing the one being re-deployed.
- **Step #6 - Removal from inventory**: The Authority is responsible for removing the equipment from departmental inventory lists as appropriate.
- **Step #7 - Redeployment to another unit**: Departments can redeploy equipment to other departments but must keep all appropriate documentation listed.
- **Step #8 - Donation**: Equipment may be donated only to non-profit organizations. No licensed software may be supplied with the equipment other than an Operating System as supplied at initial purchase.
- **Step #9 - Sale**: Equipment may be sold at fair market value to individuals, non-profit organizations or for-profit entities. This option is subject to strict rules governing the determination of fair market value, adherence to tax laws and regulations and documentation of the transaction.
- **Step #10 - Scrap & Salvage**: If the equipment is not operational or unsuitable for any use, it should be scrapped. Parts and peripherals may be salvaged. The remainder of the equipment should be disposed of as per rules. Under no circumstances is it acceptable to dispose of scrap equipment by introducing it into regular trash streams such as tossing it into the trash or dumpster. This includes hard drives removed from towers and physically destroyed.

4.2 Policy for Website & Email Management

The objective of the website is to provide a point of entry for the public to the University's officially recognized information resources through links and navigational mechanisms and to provide timely content and links to notifications, news and events of general interest about Dibrugarh University.

There are two main sections to the site:

- **The front end published site**, which is available to the public to view
- **The private back-end site**, which is available only to the authorized members of the university and accessible through valid username and password.

A Website Technical cum Monitoring Committee will be formed by the authority to get necessary suggestions regarding the website. The committee may comprise at least two technical persons from IT background.

4.2.1 Policy for Web Users:

- The Web Users should use the website for information purpose only. All Web pages, files and data within the domain of *dibru.ac.in* are the exclusive property of Dibrugarh University. They are protected by the copyright law.
- Dibrugarh University attempts to provide reliable, accurate, and correct information. However, if any inadvertent errors are found, they should be brought to the notice of the Web administrator or University authority.
- Links on some Web pages may direct your browser to a Web site that is not owned, operated, or maintained by Dibrugarh University. Dibrugarh University is not responsible for the content of these websites.

4.2.2 Policy for Content Contributors

Content Contributors shall provide accurate and up-to-date data for publishing on the website. They should keep an eye on the content provided by them and published on the website. They should immediately inform the Web Administrator if any mistake is found or addition/updating of data is necessary. The Content Contributors shall always provide the softcopy (in pdf and editable doc format) of the material or notification to be published on the website to the Web Administrator. They shall only use the Institutional email id while sending the matters for publishing. If, however, Institutional email id is not available or used, a hardcopy of the material with proper seal and signature must be sent to the Web Administrator in addition to the softcopy. In such case, the material will be published only after getting both the softcopy and hardcopy.

4.2.3 Policy for Authorized Users

The authorized users should keep their profiles up to date. While updating their profiles they shall keep it professional and only relevant information should be uploaded. They shall not upload commercial advertisements, commercial links, and materials violating Copyright law, objectionable photos or links to their profiles. While selecting fonts, colours and styles for their profiles, they should make sure that these are matched with the standard format of the website. They should keep their passwords very confidential. They should frequently change their passwords in order to secure their accounts from hackers.

4.2.4 Policy for Data Entry Operator

Data Entry Operator shall upload notifications, results, tenders, recruitment notices, news and events of the University. These are frequently updated and widely accessed contents and the Data Entry Operator should take extra care to upload the information. Common mistakes such as spelling-mistake, link mismatch, typing error etc. should be avoided. The Data Entry Operator shall report to the Web Administrator.

4.2.5 Policy for Department Web Administrators

They should keep the department profiles up to date. While updating the profiles they shall keep it professional and only relevant information should be uploaded. They should not upload commercial links or advertisements, materials violating Copyright law, objectionable photos or links to the profiles. While selecting fonts, colours and styles for the department profile, they should make sure that these are matched with the standard format of the website. The Department Web Administrator should keep their passwords very confidential. They should frequently change their passwords in order to secure their accounts from hackers The Department Web Administrator shall inform the Web Administrator when an authorized user leaves his job at the Department or gets retirement.

4.2.6 Policy for Web Developers

Since the Content Management System is developed by the Web Developers, they should monitor and scan system frequently to counter any hacking attempt. They should keep the system technologically updated and apply regular security updates, patches etc. to the applications and modules used in the system whenever necessary. They should check the server load, compatibility and configurations regularly and provide necessary support.

4.2.7 Policy for Web Administrator

Web administrator manages the Web operations component of the website. Web operations involve, but is not limited to the functions such as providing authorized access to the Website, providing technical support to the Authorized users, Department Web Administrators and Data entry Operator whenever needed, providing email ids, acting in the role of liaison between the Web Developers and other duties that ensure smooth organizational Web operations. For any major structural change in the website, the Web Administrator should consult the Website Technical cum Monitoring Committee. Any request from the departments/centres/individuals to upload their own website/software/application in the dibru.ac.in server should be forwarded by the Web Administrator to the Website Technical cum Monitoring Committee for approval.

4.2.8 Policy for Website Technical cum Monitoring Committee:

The committee shall monitor the website periodically and suggest for necessary changes in the website if any. The committee shall report the authority for any violations of the

Website and Email Policy. The committee will also discuss the matters forwarded by the Web Administrator and will take necessary action.

4.2.9 Policy for Email

The purpose of the email policy is to ensure the proper use of Dibrugarh University email system and make users aware of what Dibrugarh University deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email of the form *xyz@dibru.ac.in* which will be called Institutional or Official Email Id henceforth.

- Institutional Email ids will be provided to the Teachers, Officers, Important Offices/Branch/Sections of the University Administration and others as directed by the authority. If the Institutional email id is required for an office/branch/section of the University then one employee must be assigned as a User of that email account and shall bear the entire responsibility.
- Project Fellows and Ph. D/M. Phil Students will be provided Institutional email ids for the period of their research/project work in the University on written request duly forwarded by the Supervisor/Principal Investigator/ Head of the Department. They shall inform the Web Administrator when they complete/leave their research/project. The Supervisor/ Principal Investigator shall inform the Web Administrator in case a Project Fellow/Ph. D or M. Phil student under him/her leaves the project or research in the middle of the tenure.
- Temporary email id may be provided for events like seminars, workshops etc. with a formal request for a limited period. In this case the user of the email account should be an employee of the University. The email id will be deactivated after that period. The period may be extended on written request.
- One user will be allotted only one email id in his/her name. The user of the email id should take the responsibility of the use or misuse of the email id and he/she should not disclose the password to anyone. The Web Administrator shall have the right to de-activate multiple email ids assigned to a single user.
- The email id is valid only for the period the person is in the service of the University. When the person leaves the University, he/she should take an email clearance from the authority. The person will be given 1 (one) month time from the date of receiving email clearance application to take backup of his emails, if requested in writing. It is also the responsibility of the Department Web Administrator or the Head of the Department/Director of the Centre/ Controlling Officer to inform the Web Administrator when a person of the department/centre/branch leaves his/her job or gets retirement.
- All use of email must be consistent with Dibrugarh University policies and procedures of ethical conduct, safety, compliance with applicable laws and proper communication practices.

- Use of the Institutional Email to misrepresent the University name will be considered as misconduct.
- Engaging in unlawful or malicious activities using the Institutional email id will be considered as misconduct and shall be considered as punishable offence by law.
- Use/distribution of viruses or worms like Trojan Horse, trap-door program code, or other code of file designed to disrupt, disable, impair or otherwise harm the university network or systems is strictly prohibited.
- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language through Institutional email id shall be considered as a punishable offence by law.
- Sending or accessing pornographic/objectionable material through Institutional email id or registering to objectionable websites through the Institutional email id shall be strictly prohibited.
- It is a violation of University policy for any employee, including system administrators and supervisors, to access electronic mail and computer systems files unethically to satisfy curiosity about the affairs of others, unless such access is directly related to that employee's job duties. Employees found to have engaged in such activities shall be subject to disciplinary action.

4.3 Policy for Internet and Intranet

Dibrugarh University endeavours to provide all faculty, students and staff with a smooth and hi-speed network access provided by the National Knowledge Network (NKN), India for academic and administrative purposes. The users in the Dibrugarh University Network and IT services are expected to follow the following rules:

- Faculty, staff and students with authorized accounts may use the University Computer Network (**UCN**) and IT services for academic and administrative purposes or for personal purposes so long as such does not violate any law or policy of the University or IT Act of Government of India. It should not hamper the network speed, bandwidth or work of an academic and administrative nature.
- No commercial gain or private profit other than that allowed by the University can be made through the access of the University Computer Network
- Users are expected to respect the privacy of the other users and they may not allow any other person to use their passwords or share their account for accessing the UCN. It is the users' responsibility to protect their account from any form of phishing and from unauthorized use by others by changing their passwords periodically and using passwords that are not easily guessed. Sharing of passwords for any purpose whatsoever is strictly prohibited.

- Any attempt to circumvent system security, guess others' passwords, or in any way gain unauthorized access to local or network or IT resources is forbidden. Users are prohibited from using any false account or another person's account.
- Violations of policy will be treated as academic and administrative misconduct, or indiscipline as appropriate. Depending upon the nature of the violation, the university authorities may take an action by issuing a warning through disabling the account. In extreme cases, the account may be completely deleted and/ or the user prohibited access to IT services at university, and/ or sent to the University disciplinary action committee as constituted by the University authorities.
- The policy may change as and when it is considered appropriate and new policies or the changes in policy will take effect immediately.

4.3.1 Proxy-Server Privacy

- All users are required to access the internet through the University proxy server with proper authentication. Users are required to authenticate themselves with their passwords to be provided by the System Administrator. The passwords shall never be logged in the system/server.
- Accesses of pornographic and other offensive web-sites are blocked by the proxy-server and web-filtering software.
- The accessed pages except the email contents are cached in the system. Normally, the cached pages are neither mined nor examined. However, such examinations may be carried out for investigation of misdemeanour.
- Web access records of all users are logged for three months. Mining of the logs may be carried out to generate performance statistics and to determine the top down-loaders of the day.
- There will be a maximum download load file-size limit set in the proxy server to minimize the bandwidth consumption of the UCN. However, the maximum file-size download limit may be waived for very particular users for a limited time period on the proper consent from the authority of the University.

4.3.2 Privacy of Passwords of the UCN Users

- The passwords will be maintained in encrypted format in the server and shall be never logged unless required at all.
- The administrators may run standard password crack software on the encrypted passwords during routine security audits. Users shall be advised if their passwords are found to be weak.

4.3.3 Security

No Quality of Service guarantees for security can be given. However, the following routine precautions are to be adopted.

- Only administrators are authorized to login to the proxy and other servers.

- All ports except those necessary for functioning of the servers will be blocked (fire-walled) both from outside and inside.
- Standard intrusion detection software will be run on the LAN to monitor any change of MAC addresses corresponding to IP addresses of trusted machines.

4.3.4 Network Access and Monitoring

4.3.4.1 DHCP Server

Automatic IP addresses are allocated to the clients through the DHCP Service to access internet and other IT services. Installation of unauthorized DHCP server without the consent of the System Administrator is strictly prohibited.

4.3.4.2 Wifi Routers and Access Points

- Installation of unprotected WiFi routers is banned by the regulation of Government of India. The GOI regulation prohibits shared access of WiFi resources and mandates WiFi access only through a central authentication mechanism. In view of this, 802.1x (WPA2-Enterprise) is the minimum acceptable standard for setting up WiFi access in the university.
- Installation of WiFi routers in the academic area will not be permitted without explicit consent from the System Administrator. All users should use the authorized WiFi SSIDs for WiFi access and verify the authenticity by password.
- All WiFi routers that provide connection to the University LAN should have at least WPA2-PSK (pre-shared key with WPA2 encryption) standard security enabled.

4.3.4.3 Switches and Other Network Devices

No switches, I/O boxes, WiFi routers etc. in the various academic and administrative buildings of the University shall be handled by the individuals without the consent of the System Administrator.

4.3.4.4 Connecting other ISP networks to UCN LAN

It is strictly prohibited to connect other ISP networks to the University LAN without explicit consent from the System Administrator. In case, it is allowed due to research or operational needs it will be the responsibility of the facility in-charge to completely firewall the external network from the University VLAN, both for inward and outward connections.

4.3.4.5 VPN and *ssh* access to UCN LAN

It is strictly prohibited to setup unauthorized VPN or ssh access facilities for connecting to **UCN** LAN from outside without explicit consent from the System Administrator.

4.3.4.6 Internet Access

Access to the Internet in the university will only be available through the proxy servers. Access through the proxy servers will be restricted to ftp, http and https protocols with the secured ports. All accesses shall be logged along with the URL, time of access and uid of the user. The logs shall be maintained for a period of three months.

Connecting to the UCN WiFi for Internet access will require 802.1x authentication and all wireless network traffic shall be encrypted using WPA/WPA2 standards. All authentications shall be logged along with time of access, uid of the user, registered DHCP IP address and the MAC address of the accessing device. Internet accesses for ftp, http and https protocols shall be made available only through proxy servers. All accesses through the proxy servers shall be logged along with the URL, time of access and uid of the user.

The Policy of all accesses using wired LAN and WiFi from the Guest Houses shall be same as that of the policy for the University. However, it shall be responsibility of the In-Charge of the Guest House to verify the identity of the guest and record the mobile phone number of the guest, as per GOI guidelines, at the time of providing guest accounts. The logs shall be maintained for a period of three months.

Internet access from the hostels shall only be available through the designated proxy servers. Access through the proxy servers shall be restricted to ftp, http and https protocols All accesses shall be logged along with the URL, time of access and uid of the user. The logs shall be maintained for a period of three months.

4.3.4.7 User Account and Password to access Internet and IT Services

To access Internet and IT services, users have to enrol themselves by submitting a Form through proper channel to the Registrar, Dibrugarh University. On receiving the Form, the Network Administrator will create an account for the user and provide the user id and password for a limited time period. After that period the account will be suspended automatically. However, there would be no time limitation for the accounts of the faculty and staff during their service period in the University.

4.3.4.8 User Account Surrendering

Retiring employees and the students leaving the university (temporarily or permanently) are advised to get their accounts disabled by giving a written letter to the Registrar or the System Administrator. In case the accounts are not disabled and misused by some other person, the account holder would be legally responsible for such misuse of the account. If retiring employees and the students leaving the university (temporarily or permanently) want to retain the facility for some more period, such requests may be considered, if it is given in writing with valid justification and duly recommended by the authority.

4.3.4.9 Termination

User Accounts on network systems may be terminated or disabled with little or no notice for any of the reasons that violates the rules of IT Policy or for other inappropriate use of IT services.

4.4 Policy for Cyber Law & E-Security

Under The IT Act, 2000 as amended by Information Technology (Amendment) Act, 2008, Section 66-C is applicable and Section 419 of Indian Penal Code, 1860 is applicable. The victim of identity theft can file a complaint in the nearest police station where the above crime has been committed or where he comes to know about the crime. If crime is proved accused shall be punishable with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both. As per Section 77-B of IT Act, 2000 the above offence shall be cognizable and bailable while if Section 419 of IPC is applied along with other Sections, the said offence is cognizable, bailable, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate.

The policy will cover the following, in accordance to IT Act, 2000 as amended upto date.

E-mail Fraud: Under The IT Act, 2000 as amended by Information Technology (Amendment) Act, 2008, Section 66-C & 66-D is applicable and Sections 415 & 420 of Indian Penal Code, 1860 are applicable. He can file a complaint in the nearest police station where the above crime has been committed or where he come to know about the crime. If crime is proved accused shall be punishable with imprisonment for a term which may extend to three years and shall also be liable to the fine which may extend to one lakh rupees. As per Section 77-B of IT Act, 2000 the above Offence shall be cognizable and bailable while if Section 415 of IPC is applied for the said offence is non-cognizable, bailable, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate and Section s 420 if IPC is applied for the said offence is cognizable, non-bailable, compoundable with permission of the court before which the prosecution of such offence is pending and triable by magistrate of first class.

E-mail Spoofing: Under The IT Act, 2000 as amended by Information Technology (Amendment) Act, 2008, Section 66-D is applicable and Section 417, 419 & 465 of Indian Penal Code, 1860 are applicable. The victim can file a complaint in the nearest police station where the above crime has been committed or where he comes to know about the said crime. If crime is proved accused shall be punishable with imprisonment for a term which may extend to three years and shall also be liable to the fine which may extend to one lakh rupees. As per Section 77-B of IT Act, 2000 the above Offence shall be cognizable and bailable while if Section 417 of IPC is applied for the said offence is non-cognizable, bailable,

compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate, Section 419 of IPC is applied for the said offence is cognizable, bailable, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate, Section 417 of IPC is applied for the said offence is noncognizable, bailable, non-compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate.

Pornography: Under The IT Act, 2000 as amended by Information Technology (Amendment) Act, 2008, According to Section 67-A is applicable and Section 292/293/294, 500, 506 & 509 of Indian Penal Code, 1860 are also applicable, and the victim can file a criminal complaint in the nearest Police Station where the above crime has been committed or where he comes to know about the crime. If the crime is Proved Accused shall punishable for first conviction with imprisonment for term which may extend to Five years and with fine which may extend to ten lakh rupees and in second conviction with imprisonment for a term may extend to Seven years and with fine which may extend to ten lakh rupees. As per Section 67-A of IT Act, 2000 the above Offence shall be cognizable and non-bailable while if Section 292/293/294 of IPC is applied it will be cognizable, bailable, non-compoundable and triable by any magistrate. If Section 500 and 506 of IPC is applied it will be non-cognizable, Bailable, compoundable by the person defamed/intimidated and triable by any magistrate but if 509 of IPC is applied it will be cognizable, Bailable, compoundable by the women whom it was intended to insult or whose privacy was intruded upon and triable by any magistrate

Hacking: Under Information Technology (Amendment) Act, 2008, Section 43(a) read with section 66 is applicable and Section 379 & 406 of Indian Penal Code, 1860 also are applicable. If crime is proved under IT Act, accused shall be punished for imprisonment, which may extend to three years or with fine, which may extend to five lakh rupees or both. Hacking offence is cognizable, bailable, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate.

Spreading Worm or Virus: In most cases, viruses can do any amount of damage the creator intends them to do. They can send data to a third party and then delete the data from the computer. They can also ruin/mess up a system and render it unusable without a re-installation of the operating system. Under Information Technology (Amendment) Act, 2008, Section 43(c) & 43(e) read with Section 66 is applicable and under Section 268 of Indian Penal Code, 1860 also applicable. Spreading of Virus offence is cognizable, bailable, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate.

4.5 Policy for the protection of confidential data

4.5.1 In the case of Confidential University data, the access right will be solely with the authorised official(s) of the Dibrugarh University.

4.5.2 It is the responsibility of all the authorised user(s) to take care when handling, using or transferring confidential data so that it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data.

4.5.3 In Case Data is handled / accessed / used by any third party agent authorised by Dibrugarh University officials, it is the sole responsibility of the third party to use the data as per University norms and policies.

4.5.4 In case the confidential data is lost or stolen it must be immediately brought to the notice of the concerned authorities.

4.5.5 Personal data shall be:

a. processed fairly and lawfully.

b. processed only for specified, lawful and compatible purposes.

c. kept for no longer than necessary.

d. processed in accordance with the rights of data subjects.

e. kept secure.

f. transferred outside the Dibrugarh University Campus only if there is adequate protection.

4.5.6 Sensitive personal data may be processed in circumstances prescribed below:

a. for the prevention or detection of any unlawful act

b. for protecting the public against dishonesty or malpractice

c. for publication in the public interest

d. for providing counselling, advice or any other service

e. for research

f. for any lawful functions.

g. in the form of disclosures to elected representative

4.5.7 Because all files created or maintained using the University's Information Resources are properties of the University, it must be understood that the University can convey no expectation of privacy or confidentiality to a user. While general access to specific files can be limited or controlled where appropriate for legitimate reasons, authorized University

officials can enter and examine the contents of all files maintained on University-owned equipment.

4.5.8 It will be a crime to make unauthorized use of protected computer systems or data files on computers, or to make intentionally harmful use of such computers or data files. The seriousness of such a crime ranges from a misdemeanour to a third-degree felony. The University will prosecute all cases of unauthorized access to, or intentional damage or misuse of, University information computing resources as per law.

*****