Table of Content

(डॉ० अमित कुमार राय)
परीक्षा नियंत्रक

C.K. Dixit
Faculty of Science & Technology

Drafted by: Pooja Agarwal, System Analyst, DSMNRU.

- Internet Gateway Security

9. Network Access Policy
    - Access to Internet and Intranet
    - Access to DSMNRU's Wireless Network
    - Filtering and blocking of sites
    - Monitoring and Privacy
10. Statement of Responsibility
11. Privacy and Personal Rights
12. Email Policy
13. Social Media Sites Access Policy
14. Audit of Network Infrastructure
15. Risk Management Policy
16. Intellectual Property
17. Enforcement
18. Deactivation
19. Breach of IT Policy
20. Revision to Policy
21. Committees
    - IT Policy Advisory Committee
    - IT Policy Implementation Committee
    - IT Infrastructure Management Committee

Drafted by: Pooja Agarwal, System Analyst, DSMNRU.

(डॉ० अमित कुमार राय)
परीक्षा नियंत्रक

Prof. (Dr.) C.K. Dixit
Dean
...ty of Science & Technology

Objectives of IT Policy

The objective of this policy is to ensure proper access to and usage of DSMNRU's IT resources and prevent their misuse by the users. Use of resources provided by DSMNRU implies the user's agreement to be governed by this policy.

- University IT policy exists to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the University on the campus.
- This policy establishes University-wide strategies and responsibilities for protecting the Confidentiality, Integrity, and Availability of the information assets that are accessed, created, managed, and/or controlled by the University.
- Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information.

Scope of IT Policy

Hardware

Hardware comprises of various items that are used by the end users as well as the items that are used to support the use of IT by the end users. For example, Servers, Desktops, Laptops, Tablets, Mobile Phones, Printers, Scanners, UPSs, Network Switches, Access Points etc. and various other equipment.

Software

Systems Software comprises of software that make the system function and constitute an integral part of the system. For example, Operating System is a System Software and common applications like E-Mail Client can be considered to be an Application Software. System Software are proprietary e.g. Windows OR in Public Domain e.g. Linux. Application Software include MS-Office, MS Outlook etc. are proprietary whereas Thunderbird E-Mail, Open Office Suite etc. are Open Source Software.

As far as it is practicable and consistent with the intended purpose, Users ought to prefer Public Domain Software which is available either free OR at a much lower cost.

(डॉ० अमित कुमार राय)

Prof. (Dr.) C.K. Dixit
Dean
Faculty of Science & Technology

Drafted by: Pooja Agarwal, System Analyst, DSMNRU.

Software for Common Usage should be identified and implemented across the university in order to achieve consistency of formats and ease of sharing common data.

User

Here "user" identifies the full and part-time staff members, students, research scholars, consultants, temporaries, interns, retirees, and other users affiliated with third parties who access university technology resources, all users of IT equipment owned or leased by the University, all equipment connected to University data and voice networks etc.

Roles and Responsibilities

1) The following roles and responsibilities are envisaged from each entity respectively.
2) DSMNRU shall implement appropriate controls to ensure compliance with this policy by their users. Computer Centre shall be the primary Implementing Agency and shall provide necessary support in this regard.
3) Computer Centre shall ensure resolution of all incidents related to the security aspects of this policy by their users. Implementing Agency shall provide the requisite support in this regard.
4) Use DSMNRU's IT resources for those activities that are consistent with the academic, research and public service mission of the University and are not "Prohibited Activities".
5) All users shall comply to existing national, state and other applicable laws.
6) Abide by existing telecommunications and networking laws and regulations.
7) Follow copyright laws regarding protected commercial software or intellectual property.
8) As a member of the University community, DSMNRU provides use of scholarly and/or work-related tools, including access to the Library, certain computer systems, servers, software, databases and the Internet. It is expected from University Community to have a reasonable expectation of unobstructed use of these tools, of certain degrees of privacy and of protection from abuse and intrusion by others sharing these resources. Authorized users can expect their right to access information and to express their

Drafted by: Pooja Agarwal, System Analyst, DSMNRU.

(डॉ० अमित कुमार राय)
परीक्षा नियंत्रक

Prof. (Dr.) C.K. Dixit
Dean
Faculty of Science & Technolo

opinion to be protected as it is for paper and other forms of non-electronic communication.

9) Users of DSMNRU shall not install any network/security device on the network without consultation with the Implementing Agency.
10) It is responsibility of the University Community to know the regulations and policies of the University that apply to appropriate use of the University's technologies and resources. University Community is responsible for exercising good judgment in the use of the University's technological and information resources. Just because an action is technically possible does not mean that it is appropriate to perform that action.
11) As a representative of the DSMNRU community, each individual is expected to respect and uphold the University's good name and reputation in any activities related to use of IT communications within and outside the university.
12) Competent Authority of DSMNRU should ensure proper dissemination of this policy.

IT Management Policy

Maintenance/Upgradation Policy

- On procurement & installation of any new IT device/equipment, User department must allocate a unique dead-stock number (Asset Identification Number) in the deadstock/Asset Register. The same number must be written on the front side of the device/equipment, which can be used for physical verification. The same must be appropriately updated while transferring out or disposing/writing off such assets.
- User department must be vigilant about warranty checks and must take appropriate action if the performance of the device/equipment deviates from the expected performance.
- After the completion of the warranty period, User Department may implement the Annual Maintenance Contract (AMC) for the device/equipment depending on the criticality of its usage, with the approval of the IT Infrastructure and Management Committee & following the standard procedure laid down by the university from time to time.

(डॉ० अमित कुमार राय)
परीक्षा नियंत्रक

Prof. (Dr.) C.K. Dixit
Dean
Faculty of Science & Technology

Drafted by: Pooja Agarwal, System Analyst, DSMNRU.

- The IT Infrastructure and Management committee shall define, review, revise, approve and circulate/publish the guidelines & procedure for up-gradation of outdated IT devices/equipment's/components or to improve the performance of existing IT devices/equipment's/components and software. The upgradation of devices/equipment's can be through increasing the performance capacity by adding/replacing some components, like memory, HDD, Graphic card etc. or by replacing the whole device/equipment through a buy-back mechanism depending on the specifications and performance parameters of the device/equipment. A prior approval of specifications and requirement by the IIM Committee is essential.
- Necessary budget provisions must be made by the respective user departments for the maintenance and up-gradation of its IT equipment and software.

IT equipment Disposal-off/Write-off Policy

- IT Infrastructure Management Committee (IIM Committee) is responsible to define, review, revise, approve and circulate/publish the guidelines & procedure to scrap and write off the non-functional, non-operable, non-repairable and obsolete IT devices/equipments.
- It must perform the vendor evaluation and registration process to identify & register the vendors specialized in disposal of e-scrap or digital scrap.

Budgetary provisions for IT

- Budgetary provisions should be made under recurring grants (OPEX) to maintain all the existing IT infrastructure for smooth functioning of all the IT enabled services.
- Adequate budgetary provisions under capital head (CAPEX) should be kept for upgradation and augmentation of IT infrastructure
- Budgetary provisions under capital grants should also be allocated for implementation of newer IT solutions from time to time.
- In DSMNRU, there has been an increase of 10% enrolment of students every year. Keeping in view of this increase and for the benefit of the students, a budget of 10% of the total budget of the university should be earmarked for IT facility particularly for students

(डॉ० अनिल कुमार राय)
परीक्षा नियंत्रक

Prof. (Dr.) C.K. Dixit
Faculty of Science & Technology

Drafted by: Pooja Agarwal, System Analyst, DSMNRU.

IT Usage Policy

- An authorized user may use only the IT resources he/she has authorization. No user should use another individual's account, or attempt to capture or guess other users' passwords.
- A user is individually responsible for appropriate use of all resources assigned to him/her, including the computer, the network address or port, software and hardware.
- Therefore, he/she is accountable to the University for all use of such resources. As an authorized DSMNRU user, he/she should not engage in or enable unauthorized users to access the network by using IT resources of DSMNRU or a personal computer that is connected to the DSMNRU campus wide Local Area Network (LAN).
- The university is bound by its End User License Agreement (EULA), respecting certain third party resources; a user is expected to comply with all such agreements when using such resources.
- Users should make a reasonable effort to protect his/her passwords and to secure resources against unauthorized use or access. No user must attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system owner or administrator.
- Users must comply with the policies and guidelines for any specific set of resources to which he/she have been granted access.
- When other policies are more restrictive than this policy, the more restrictive policy takes precedence.

Fair / Ethical Usage Guidelines

- All users are expected to make use of the IT resources accessible to them with sensibility and awareness.
- The DSMNRU-Intranet and Internet access will not be used for commercial activity, personal advertisement, solicitations, or promotions, such as hosting or providing

(डॉ० अमित कुमार राय)
परीक्षा नियंत्रक

Prof. (Dr.) C.K. Dixit
Dean
Faculty of Science & Technology

Drafted by: Pooja Agarwal, System Analyst, DSMNRU.

links of commercial websites or email broadcasts of commercial promotions to the users.

- Any part/component of the IT infrastructure of the university shall not be misused for Anti-University, Anti-State or Anti-Government activities. The IT Policy Implementation Committee will be authorized to undertake appropriate measures to ensure maintenance of such discipline and initiate suitable actions for prevention of such undesirable activities.
- As such, non-DSMNRU organizations (such as commercial outlets operating on the DSMNRU campus, IGNOU, GSLET etc.) will not be connected to the DSMNRU-Intranet, and cannot be a part of the DSMNRU domain space.
- The downloading of audio and video files is to be done strictly for official purposes.
- f. Each user must preserve & maintain the confidentiality of the password used by him/her. No user must try to access the IT resources using other user's password, either knowingly or otherwise.
- Access to sites that are banned under law or that are offensive or obscene is prohibited. This is also an offence under the Indian IT Act 2000 and attracts severe punishment.
- Use of the network to tamper with information on other computers, to deliberately spread harmful/pirated programs, compromise other systems, or to cause damage of any kind using the intranet/internet is prohibited, and is an offence under the Indian IT Act 2000. The user is liable for any civil losses caused, in addition to criminal prosecution under the Indian IT Act 2000.
- No equipment/user other than those registered with the University, can be used to connect to the intranet.

Centralized Authentication of Users

- Computer Centre is responsible to devise a mechanism for management of registration and access policy for all users using, for example, LDAP or Active Directory or any other appropriate software. It should provide a GUI based platform for user administration through which user departments can administer their users in the centralized database of users in LDAP or Active Directory. The head of every

(डॉ० अविनि कुमार राय)
परीक्षा नियंत्रक

Prof (Dr.) C.K. Dixit
Dean
Faculty of Science & Technology

Drafted by: Pooja Agarwal, System Analyst, DSMNRU.

user department is responsible to add/modify the information about its users and their access rights on centralized user database managed by Computer Centre. The head may designate a staff member, preferably a permanent staff member, to assist him/her for the user information management of its users on the central user database and inform the Computer Centre about the same.

- Computer Centre under the guidance and support of the IT Policy Implementation Committee shall provide necessary training to all heads and designated staff members to manage the user information of their respective user department.
- The user department shall update information of its students after finalization of admissions once every year. The modification of user data for teaching/non-teaching staff and any other user must be updated immediately by the user department with the change in the user status. Individual user is not responsible for updating of his/her information in the user database.
- The IT Policy Implementation Committee shall have an authority to override such permissions granted in case of any user.

Sharing of hardware resources like desktops, printers, scanners etc. by employees

- IT resources are limited and users are more. Hence, the resources have to be shared sensibly and effectively.
- Use of network Office equipment like Network Printers and Network Scanners should be encouraged.
- Minimum computer-student ratio of 1:2 in every teaching department offering IT programs / courses and a ratio of 1:4 to 1:6 in non-IT programs/courses is desirable.
- A desirable Computer-staff ratio of 1:2 should be maintained in research departments/institutions. A desirable Computer-staff ratio of 1:3 should be maintained in all other non-teaching / administrative departments/sections/offices.
- Due care should be taken not to overwrite / delete other users' data on shared resources. In case of any difficulty, guidance and support can be taken from the Computer Centre.

Drafted by: Pooja Agarwal, System Analyst, DSMNRU.

(डॉ० अमित कुमार राय)
परीक्षा नियंत्रक

Prof. (Dr.) C.K. Dixit
Dean
Faculty of Science & Technology

IT Security Policy

Physical Security of Servers, Desktop, Laptop, Thin client, Portable Devices etc.

- The user department where the IT equipment is installed and used, either temporarily or permanently, is responsible for the physical security of it.
- It is responsible for allowing the physical access to the IT resources only to authorized users.
- It is also responsible to ensure proper power supply with effective grounding (earthing), proper furniture as well as cleanliness of the equipment and environment including air-conditioning machines.
- The user department must ensure proper load on electricity meter before installing additional IT equipment or other allied equipment's like air-conditioning machines etc. The user department must get the power load on electricity meter checked by MGVC every 2 years. The power load on electricity meters must be calculated and increased taking into account requirements of next 2 years.
- Users of a user department can access the network via desktop/laptop computers on the campus network. Users are responsible and accountable for the usage of the systems allocated to them.
- Users must take adequate & appropriate measures to prevent misuse of network from computer systems that they are responsible for.
- Individual users as well as User departments should take reasonable care of the vulnerability of systems attached to the campus network. In particular, users must apply appropriate service packs, browser updates and antivirus and client security solutions in their MS Windows machines, and necessary upgrades, OS patches, browser updates etc. for other systems.
- If a user department wishes to set up its own Internet access facility, then it should be done under support and monitoring of the Computer Centre and ensure that deploying such an access facility does not jeopardize the security of the campus network. The user department must completely adhere to the provisions of this IT Policy for such facility.

(डॉ अमित कुमार राय)
विभाग निदेशक

Prof. (Dr.) C.K. Dixit
Dean
Faculty of Science & Technology

Use of Licensed Software

- Software programs are covered by copyrights and a license is required for their use.
- Legal, free and compatible alternatives are available for a large number of applications / software and users must evaluate them, rather than straightway going for software having a cost.
- Users / User departments must ensure that they have either an academic, commercial or public license (as in the case of 'free' software) for any software they install on the systems that they are responsible for.
- Use and exchange of pirated / illegal software over the DSMNRU-Intranet is prohibited. It is the responsibility of the head of the user department to ensure compliance.
- The downloading and use of software that is not characterized as public domain or 'free' is prohibited.
- Use of Open Source Software is encouraged to avoid financial burden and legal complications arising out of license management. For example, use of Kingsoft Office or Open Office must be preferred over MS-Office, Thunderbird E-Mail Client as against MS Outlook.
- Computer Centre should arrange for the training of general purpose Open Source Software for all the users.

Use of Antivirus & Internet/Endpoint Security/Protection Software

- The user department is responsible for installation and maintenance of proper Anti-virus or Internet/Endpoint Security/Protection Software or any other security software as prescribed by the IT infrastructure Management Committee.
- In case of detection of any issues in the security, the compromised computer/equipment must be disconnected from the DSMNRU-Intranet failing which Computer Centre shall disable the respective network connection.
- Strict action may be taken by the IT Policy Implementation Committee against users who deliberately prevent installation of such security software OR disable such software OR prevent them from running.

Prof. (Dr.) C.K. Dixit
Dean
Faculty of Science & Technology

Drafted by: Pooja Agarwal, System Analyst, DSMNRU.

Information Security Policy

Definition of Critical Information

- Restricted Information, which is highly valuable and sensitive. The unauthorized alteration, disclosure or loss of this information can cause significant damage (devastating) to the university, for example, examination results under process, accounts etc. This information must be highly protected as it cannot be easily recovered or brought to its original state easily.
- Private Information, which is of moderate importance and sensitivity. Its unauthorized alteration, disclosure or loss of this information can cause moderate damage to the university. Generally, the information which is not classified in other two classes falls under this. Reasonable and effective security is required for this information, as recovery of its original state may take sizable amount of resources.
- Public Information, which is of low importance and sensitivity. Its unauthorized alteration, disclosure or loss of this information can cause little damage to the university. Public information includes press releases, circulars, notifications, course information and research publications, published results on website etc. While little or no controls are required to protect the confidentiality of Public information, some level of control is required to prevent unauthorized modification or destruction of Public information.
- All information created, processed, generated, maintained and deleted by the university must be classified into these categories and different levels of user privileges must be defined for each function. Only authorized users can get access to the category of information he/she is authorized to access.

Backup Policy

- Every user and user department should manage & maintain backup of data stored on the computers under their control based on its level of criticality. Daily/twice a day /thrice a day backup of Restricted Information must be taken depending on its frequency of updates. The backup of server data must be maintained on designated desktop computers by increasing its storage capacity, on regular basis to prevent any data loss in certain incidents.

(डॉ० अशोक कुमार राय)
परीक्षा नियन्त्रक

Prof. (Dr.) C.K. Dixit
Dean
Faculty of Science & Technology

Drafted by: Pooja Agarwal, System Analyst, DSMNRU.

- Backup of official data on laptops, external hard drives or any other mobile/removable media should be discouraged.
- Backup or temporary storage of official data on free public cloud storage facilities like DropBox, Google Drive, OneDrive etc. is unsafe and prohibited.
- No user/user department should take official data outside the DSMNRU campus without necessary authorization.
- Computer Centre should provide Centralized storage facility for all user departments to store backup of their official data only on DSMNRU-intranet. No access to this backup shall be allowed from internet outside the campus. User departments can store ONLY OFFICIAL AND CRITICAL information using the centralized backup solution. A backup of Critical / Confidential Information SHOULD BE stored in the local Hard Disk as well as on removable media which may be stored in fire-proof/water-proof safes at different locations to protect critical data from manmade or natural calamities.
- Periodicity of the backup should be decided based on the level of criticality of information.
- Information should be classified based on its level of criticality. Users with special privileges should have the accessibility of different levels of critical information.

Network Management and Security Policy

Structure of DSMNRU-Intranet Wired & Wireless

The DSMNRU-Intranet consists of about 4000 nodes connected through UTP structured cabling with a layered architecture of L3, L2 and EDGE switches with an optical fiber cable backbone of more than 25 KMs. across the campuses. In 2013, a campus-Wi Fi project was implemented by Faculty of Science & 5 different faculties and campuses are covered under campus-Wi Fi, namely, Faculty of Science, Faculty of Technology & Engineering, Faculty of Family and Community Sciences and Girls' Hostels, Polytechnic College & Boys' Hostels and University Head Office and Boys' Hostels in the first phase. Remaining campuses shall be covered under Campus-WiFi gradually.

(डॉ० अनिल कुमार राय)
परीक्षा नियन्त्रक

Prof. (Dr.) C.K. Dixit
Dean
Faculty of Science & Technology

Drafted by: Pooja Agarwal, System Analyst, DSMNRU.

- The Computer Centre is the nodal agency responsible for establishment, maintenance and management of the campus-LAN. All the technical aspects of network related activity like, defining specifications of network components, establishment, maintenance
- and management of wired and wireless LAN, strategic planning for expansion of LAN, management of internet bandwidth and gateway, Network Security Management, implementation and coordination of government sponsored schemes like NMEIT and NKN etc. is the sole responsibility of the Computer Centre.
- Computer Centre is responsible for the core DSMNRUB network (includes Internet facilities: email, web etc).
- Computer Centre will provide connectivity to each User Department, to the gigabit backbone, and also the necessary IP addresses, proxies, email relays etc.
- If any node or part of DSMNRU-Intranet "misbehaves" and causes problems for any other user department or the entire campus, or disrupts services, Computer Centre will notify the concerned Head and disconnect the node or part of DSMNRU-Intranet from the core network until the problem is fixed satisfactorily.
- Computer Centre will decide which web sites can be accesses through the campus internet and, shall disallow access to other sites and maintain a mechanism suitable to enforce such a purpose under the guidance and supervision of IT Policy Implementation Committee
- University has been provided 1Gbps internet connectivity through National Knowledge Network (NKN) upto 2020. This will eventuality be upgraded to 10 Gbps by NKN. University has also installed a backup connectivity of 10 Mbps from BSNL. This is sufficient for the internet requirements for the university. Therefore, the requirement for a separate Leased Line or Broadband internet connectivity must be discouraged. However, any such facility has been installed by any user department of the university, it has to comply with all the provisions of the IT Policy.

(डॉ० अमित कुमार राय)

Prof. (Dr.) C.K. Dixit

Faculty of Science & Technology

Drafted by: Pooja Agarwal, System Analyst, DSMNRU.

Methodology of Implementation & Expansion of LAN Including Campus Wi-Fi

- Computer Centre should define and implement the best methodology for optimum implementation and effective utilization of the campus-LAN. It should define the standard specifications for laying of OFC, structured UTP cabling and wi-fi for optimum network performance with the approval and certification of the IT Infrastructure Management Committee
    - Standards and specifications for laying OFC (to be defined)
    - Standards and specifications for structured UTP cabling (to be defined)
    - Standards and specifications for campus-wifi (to be defined)

Maintenance of DSMNRU-Intranet including Routers, Switches, Cabling, Access Point etc. AMC

- Maintenance of active & passive network components is very important for the health and performance of any network.
- Routers, core switches are costly components and need to be taken care of well.
- Only manageable switches and components including APs should be used. Use of unmanaged network components is strictly prohibited.
- Proxy Servers and DHCP servers shall be configured and maintained by the Computer Centre only. However, any user department wanting to configure its own DHCP server and use its own range of IP addresses must use the IP range other than DSMNRU-Intranet and communicate all the configuration details of its VLAN to the Computer Centre.
- Use of open proxy servers or any other mechanism to bypass the defined security configurations at any level without prior permission from the IT Infrastructure Management Committee under intimation to Computer Centre shall be treated as breach of policy and dealt with strictly.
- Any user department wishing to use live IP addresses for its applications shall have take written permission from IT Infrastructure Management Committee receiving on which Computer Centre shall allocate live IPs in writing to the user department. It shall be the sole responsibility of the user department to ensure that no security or

Prof. (Dr.) C.K. Dixit
Dean
Faculty of Science & Technology

Drafted by: Pooja Agarwal, System Analyst, DSMNRU.

operational difficulties/threats are created in DSMNRU-Intranet. Computer Centre shall maintain the records of all live IP addresses.

- The respective user departments must take care of network components installed in their premises and ensure physical security of them. The user department should also provide adequate power supply for network devices in stalled in its premises.
- Computer Centre should be given separate budgetary provisions for network maintenance.
- Wired and wireless networks should be kept separate for more efficient network management.
- User departments must cooperate in providing necessary space and power supply for installation of network components/devices at technically appropriate place defined by Computer Centre in their premises.
- Computer Centre will evaluate, procure and deploy and appropriate Network Management Software Application to ensure its uptime, security, efficiency and effectiveness.

Bandwidth Management

Network Management is one of the core functions of the Computer Centre. University has 1Gbps internet bandwidth through NKN. Distribution of the bandwidth across the campus-LAN is a very important aspect of bandwidth management. The bandwidth management should give priority to academic contents, Application Software implemented by the university, research projects, University Website & E-mail facility etc. over general internet browsing and other utilities.

Internet Gateway Security

Securing Internet Gateway is a very challenging task. Computer Centre is solely responsible to ensure effective security of the gateway. Enterprise Firewall or Unified Threat Management Solution must be implemented effectively with strong policy definitions in line with IT policy of the university. University Administration must provide an active administrative support to secure the internet gateway by the Computer Centre.

(डॉ० अमित कुमार राय)
परीक्षा नियंत्रक

Prof. (Dr.) C.K. Dixit
Dean
Faculty of Science & Technc

Drafted by: Pooja Agarwal, System Analyst, DSMNRU.

Network Access Policy

Access to Internet and Intranet

- A user shall register the client system and obtain one-time approval from the competent authority before connecting the client system to the University Campus wide LAN.
- DSMNRU shall maintain two independent networks, i.e. Internet and Intranet. Both the networks shall not have any physical connection/devices between them. End point compliance shall be implemented on both the networks to prevent unauthorized access to data.
- Users shall not undertake any activity through any website or applications to bypass filtering of the network or perform any other unlawful acts which may harm the network's performance or security.

Access to DSMNRU's Wireless Networks

For connecting to a DSMNRU's wireless network, user shall ensure the following:

- A user shall register the access device and obtain one-time approval from the competent authority before connecting the access device to the DSMNRU's wireless network.
- Wireless client systems and wireless devices shall not be allowed to connect to the DSMNRU's wireless access points without due authentication.
- To ensure information security, it is recommended that users should not connect their devices to unsecured wireless networks.

Filtering and blocking of sites

- Computer Centre or any other Implementing Agency (IA) may block content over the Internet which is in contravention of the relevant provisions of the IT Act 2000 and other applicable laws or which may pose a security threat to the network.
- Computer Centre or any other Implementing Agency (IA) may also block content which, in the opinion of the university, is inappropriate or may adversely affect the productivity of the users.

Prof. (Dr.) C.K. Dixit
Dean
Technology

Drafted by: Pooja Agarwal, System Analyst, DSMNRU.

Monitoring and Privacy

- Computer Centre or any other Implementing Agency (IA) shall have the right to audit networks and systems at regular intervals, from the point of compliance to this policy.
- Implementing/Nodal Agency, for security related reasons or for compliance with applicable laws, may access, review, copy or delete any kind of electronic communication or files stored on University provided devices under intimation to the user. This includes items such as files, e-mails, posts on any electronic media, Internet history etc.
- Implementing agency may monitor user's online activities on University network, subject to such Standard Operating Procedures of GoI norms.

Statement of Responsibility

- User Department is responsible for security of IT infrastructure & resources under its control and usage. One permanent staff member shall be designated to supervise and help maintain the IT security through coordination, guidance and training with the Computer Centre.
- Computer Centre is responsible to provide guidance and training to all user departments in maintaining due security of IT infrastructure. It is also responsible to assist IT Policy Implementation Committee in monitoring the implementation of IT policy on DSMNRU campus.
- University Administration is responsible to provide necessary administrative and financial support to ensure the IT infrastructure and resources required for implementation of IT policy.
- In the eventuality of cyber attack/crime/fraud or any other cyber security incident on or using IT infrastructure of the university, affected department/section/institution shall perform technical/legal procedure in technical coordination with Computer Centre, IT Policy Implementation Committee and guidance of Legal Cell of the university. In case of state level or national level cyber security issue, full cooperation of the user department, Computer Centre and IT Policy Implementation Committee shall be

(डॉ० अमित कुमार राय)

Prof. (Dr.) C.K. Dixit
Dean
Faculty of Science & Technology

Drafted by: Pooja Agarwal, System Analyst, DSMNRU.

extended to the Cyber Crime Cell of the Government, CERT-IN, CBI, NIA and other agency authorized by the state or central government.

Privacy and Personal Rights

- All users of the university's IT resources are expected to respect the privacy and personal rights of others.
- Do not access or copy another user's email, data, programs, or other files without authorization and approval of the Competent Authority (CA).
- While the University does not generally monitor or limit content of information transmitted on the campus wide LAN, it reserves the right to access and review such information under certain conditions after due approval of the competent authority

E-mail Access Policy

Electronic Mail is a tool provided by the University and serves as a primary means of communication and to improve education and administrative efficiency. Users have the responsibility to use this resource in an efficient, ethical and lawful manner. Use of University Email Accounts evidences the user's agreement to be bound by this policy.

a) Directorate provides the email accounts to staff and research scholars on dsmnru.ac.in domain on.

b) All staff, in particular administrative, academic and research staff should maintain and use only University email accounts and not use any external/personal account to conduct the official communications of the university.

c) The University's email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments.

d) University employees' e-mail addresses are not confidential. Employee e-mail addresses will be visible to other University e-mail account holders.

e) E-mail sent by the University to a University e-mail account is an official form of communication to employees. It is the responsibility of employees and students to receive such communications and to respond to them as may be necessary.

(डॉ० जगदीश कुमार राय)

Prof. (Dr.) C.K. Dixit
Dean
Faculty of Science & Technology

Drafted by: Pooja Agarwal, System Analyst, DSMNRU.

f) Official Communications may be time-critical and employees and students are expected to review messages sent to their University e-mail account on a reasonably frequent and consistent basis.

General Standards of Use

E-mail facility provided by the University should not be used:

- For the creation or transmission of material that is abusive or threatening to others, or serves to harass or bully others.
- For the creation or transmission of material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs.
- For activities that violate the privacy of other users.
- For the creation or transmission of anonymous messages, i.e. without clear identification of the sender.

Social Media Sites Access Policy

1) Use of social networking sites by DSMNRU users is governed by "Framework and Guidelines for use of Social Media for Government Organizations".

2) User shall comply with all the applicable provisions under the IT Act 2000, while posting any information on social networking sites.

3) User shall adhere to the "Terms of Use" of the relevant social media platform/website, as well as copyright, privacy, defamation, contempt of court, discrimination, harassment and other applicable laws.

4) User shall report any suspicious incident as soon as possible to the competent authority.

5) User shall always use high security settings on social networking sites.

6) User shall not post any material that is offensive, threatening, obscene, infringes copyright, defamatory, hateful, harassing, bullying, discriminatory, racist, sexist, or is otherwise unlawful.

7) User shall not disclose or use any confidential information obtained in their capacity as an employee of the university.

(डॉ० अमित कुमार राय)

Prof. (Dr.) C.K. Dixit
Dean
Faculty of Science & Technology

Drafted by: Pooja Agarwal, System Analyst, DSMNRU.

8) User shall not make any comment or post any material that might otherwise cause damage to DSMNRU's reputation.

Audit of Network Infrastructure

The security audit of DSMNRU network infrastructure shall be conducted periodically by an organization approved by the university.

Risk Management Policy

1) A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality and authority of University's data.

2) Implementing agency reserves the right to deactivate/remove any device from the network if it is deemed as a threat and can lead to a compromise of a system under intimation to the competent authority of the university.

3) Any security incident noticed must immediately be brought to the notice of the Indian Computer Emergency Response Team (ICERT) and the Implementing agency.

4) Notwithstanding anything in the above clause, the disclosure of logs relating to or contained in any IT Resource, to Law Enforcement agencies and other organizations by the Implementing agency shall be done as per the IT Act 2000 and other applicable laws.

5) Implementing agency shall neither accept nor act on the request from any other organization, save as provided in this clause, for scrutiny or release of logs.

Intellectual Property

Material accessible through the DSMNRU's network and resources may be subject to protection under privacy, publicity, or other personal rights and intellectual property rights, including but not limited to, copyrights and laws protecting patents, trademarks, trade secrets or other proprietary information. Users shall not use DSMNRU's network and resources in any manner that would infringe, dilute, misappropriate, or otherwise violate any such rights.

(डॉ० अमित कुमार राय)
परीक्षा नियंत्रक

Prof. (Dr.) C.K. Dixit
Dean
Faculty of Science & Technology

Drafted by: Pooja Agarwal, System Analyst, DSMNRU.

Enforcement

1) This policy is applicable to all the users of as specified in Section 2 of this document. It is mandatory for all users to adhere to the provisions of this policy.

2) Each entity of DSMNRU shall be responsible for ensuring compliance with the provisions of this policy. The Implementing Agency would provide necessary technical assistance to the user entities in this regard.

Deactivation

In case of any threat to security of DSMNRU's systems or network from the resources being used by a user, the resources being used may be deactivated immediately by the Implementing agency.

2) Subsequent to such deactivation, the concerned user and the competent authority of the university shall be informed.

Breach of This Policy

Users are encouraged to be vigilant and to report any suspected violations of this Policy Immediately to the IT Helpdesk admin@dsmnru.ac.in. On receipt of notice (or where the University otherwise becomes aware) of any suspected breach of this Policy, the University reserves the right to suspend a user's access to University's Data.

If any breach of this Policy is observed, then (in addition to the above) disciplinary action up to and including dismissal in the case of Staff, expulsion in the case of Students or contract termination in the case of third parties may be taken in accordance with the University's disciplinary procedures.

Revisions to Policy

The University reserves the right to revise the terms of this Policy at any time. Any such revisions will be noted in the revision history of the policy, which are available on the DSMNRU website and by continuing to use the University's IT Resources following any update it is considered acceptance on the revised terms of this Policy.

(डॉ० अमित कुमार राय)
परीक्षा नियंत्रक

Prof. (Dr.) C.K. Dixit
Dean
Faculty of Science & Technology

Drafted by: Pooja Agarwal, System Analyst, DSMNRU.

Committees

IT Policy Advisory Committee

IT Policy Advisory Committee (ITPAC) is responsible for creating, reviewing and recommending the IT Policy for the university.

The main functions of the committee shall be as follows.

- To define, review and recommend IT policy and modifications in the policy
- To define the standard formats to collect data/feedback of various IT functions of the university quarterly/half yearly, which can be useful to analyze and review various IT functions, including Information & Network Security.
- To ensure the effective implementation of the IT Policy defined & approved by the university syndicate. It shall also look after the web content management for the university/Faculty/Institute.

IT Infrastructure Management Committee

IT Infrastructure Management Committee (IIM Committee) is responsible to define, approve & circulate the specifications of all IT equipment requirements once in every year. The committee should meet once every month before the purchase committee.

This committee encompasses all the functions and composition of the present Computer Expert Committee. Hence, the present Computer Expert Committee should be reframed in tune with the provisions of the IT Policy by university syndicate.

The principal functions of the committee shall be as follows.

- To define, approve and circulate Standard, minimum, generic specifications of commonly used IT equipments Vendor Registration & Evaluation Standardization of procurement process – quotation & tender documents with uniform and consistent terms & conditions in concurrence with the purchase policy of the university
- To define guidelines for maintenance of separate Dead Stock register (Asset Register) for IT equipments.
- To define guidelines for management of licenses of various software – Procurement, licenses, Record Maintenance, upgrades, agreements etc.

Prof (Dr.) C.K. Dixit
Dean
Faculty of Science & Technology

- To define guidelines for management of Memorandum of Understanding (MoU) / Service Level Agreement (SLA) with hired IT solution providers, Annual rate Contract (ARC), Annual Maintenance Contract (AMC), Campus Agreement etc. related to IT Software, Applications & Equipments.
- Software procurement policy & use of Open Source Software.
- To define guidelines for document tendering or e-Tendering process for IT equipments/solutions
- To define guidelines for writing off obsolete/outdated IT hardware & software.
- Annual Internal Audit for verification of regular upkeep of the IT infrastructure by the User Departments under their control, Network Performance and Security Audit and Information Security Audit
- As regards procurement of Materials related with IT, the following standardizations should be considered:
    - Identification of Items generally being purchased regularly – for example, servers, Desktop PCs, Laptops, Printers, consumables etc.
    - Identification of a few selected Brands of these items
    - Identification of a few selected vendors who supply these brands.
    - Working out (preferably three) sets of configurations from bare minimum to the highest possible level, against which the specific requirements may be matched and the appropriate configuration meeting the requirements may be identified.
    - The procurement may be carried out from the identified vendors for the selected configuration.
    - This will help in procurement of items that fulfill the requirements with desired level of performance without unnecessarily increasing the investment due to an unduly higher configuration.
    - IT equipment & software procurement sub-committee and IT equipment & software write-off sub-committee can be constituted from the members of the IIM committee.

(डॉ० अमित कुमार राय)
परीक्षा नियंत्रक

...K. Dixit
Faculty of Science & Technology

Drafted by: Pooja Agarwal, System Analyst, DSMNRU.