दून विश्वविद्यालय
मोथरोवाला रोड, केदारपुर, पो०ओ० डिफेन्स कालोनी,
देहरादून–248001(उत्तराखण्ड) भारत

DOON UNIVERSITY
Mothrowala Road Kedarpur, P.O. Defence Colony,
Dehradun-248001 (Uttarakhand) INDIA.

(**The logo downloaded from internet, might be protected by copyright...It is needed to be designed for Doon university separatly)

IT Policy & Maintenance Policy

of

Doon University

Tel.: +91-135-2533136 (O), 2533115 (Telefax) E-mail : regoffice@doonuniversity.ac.in

दून विश्वविद्यालय DOON UNIVERSITY
मोथरोवाला रोड, केदारपुर, पो०ओ० डिफेन्स कालोनी, देहरादून–248001 (उत्तराखण्ड) भारत
Mothrowala Road Kedarpur, P.O. Defence Colony, Dehradun-248001 (Uttarakhand) INDIA.

INFORMATION TECHNOLOGY INFRASTRUCTURE USAGE AND MAINTENANCE POLICY

Introduction

In order to maintain the usefulness and flexibility of the system and to safeguard student, faculty and staff's privacy and work product, the following rules must be followed by students, teaching and non-teaching staff, management, visiting guests, and research fellowship members of University and other stake holders:

1. General Rules

1. Students, faculty, staff, management, guests and research fellows insofar as such use does not contravene any laws or university policies, members are permitted to utilize the computing, networking, and other IT facilities for academic purposes, official university business, and for personal purposes.

2. Sending, viewing, or downloading fraudulent, harassing, obscene, threatening, or any email, messages or materials that are against the law or against University policy is prohibited by the university. Therefore, user inhibition is requested in situations where the category of a certain piece of content may be questionable, such as when the content is obtained by email, etc. Any effort to undermine or misrepresent a supportive learning or working environment is, generally speaking, forbidden.

3. No user should ever intentionally or unintentionally try to alter, alter, or vandalise any data. All of its users must uphold the fundamental idea of an information resource's reliability. It is a clear violation of university policy to interfere with, disrupt, or trespass upon university IT resources.
4. No user should ever intentionally or unintentionally attempt to alter the availability of an IT resource.

5. Users must adhere to all intellectual property rights (IPR), copyright, and licencing laws and regulations when using software and materials that are protected by IPR. Any illicit file-sharing and the use of any unauthorised, pirated, or unlicensed software is strongly forbidden and is considered a violation of university policy. This includes the use of privately held IT resources while using institutional IT rights.

6. Users are barred by the university from obtaining or facilitating unauthorized access to restricted IT resources on the university network. Any such attempt would not only be against university policy, but it might also be against national and international cyber laws, The Information Technology Act of India provisions, and the fundamentals of national cyber security policy. The user would be held accountable on both a civil and criminal level. However, the University retains the full right to alone or in conjunction with its affiliates use the IT resource and Information for any legal or institutionally authorized operation.

REGISTRAR
DOON UNIVERSITY
DEHRADUN (INDIA)

7. Additionally, the university advises its employees, teachers, and students to use Processing Software (PS) and Open Source Operating Systems (OS), such as Ubuntu/ CentOS or other and Libra Office/ OpenOffice/ WPS Office, respectively. Additionally, users of computers directly or indirectly supported by Doon University should switch to the suggested OS & PS as their primary software and build competence on it. If such an adaptation has technological limitations, a justified request for a relaxation may be made to the appropriate authority.
8. Users are required to follow by the rules set forth by the relevant social networking websites, mailing lists, chat rooms, blogs, and other online media forums by consenting to the terms of use of those forums. No user should try to access information and reveal it to themselves or other unauthorised users unless they have the right authority. Each user is required to respect the bigger picture of data privacy.
9. For as long as Doon University's various departments, hostels, and other units can maintain consistency in adherence to the IT (Usage) Policy, they are free to set and enforce additional "conditions of use" for IT resources that are under their management. The Units will be in charge of making these terms of use known and enforcing them. When using external networks, appropriate policies can be applied in accordance with the general rights granted by the university's (Usage) Policy.
10. Policy violations shall be dealt with as academic dishonesty, a misdemeanor, or indiscipline, as necessary. The University authorities may take measures based on the type of infringement.
11. The University may be required to disclose to third parties, in whole or in part, its IT information, resources, and/or records as part of specific investigation procedures. Additionally, the University may evaluate, analyze, and audit its information records without prior notice to its Users in order to ensure effective monitoring and optimal use of University IT resources. In addition, the University might use services from independent service providers. Users of the University's IT resources can, therefore, only have a reasonable expectation of privacy.
12. Users are expected to maintain the equipment properly and report any malfunctions to the on-duty staff or the facility manager. The systems should not be moved, repaired, reconfigured, modified, or attached to external devices by users.
13. No food or drink is permitted in the faculty offices, classes and laboratories. Additionally, it's against the law to make noise by loud chatting, singing, or playing loud music, videos or movies (this list is not all-inclusive).
14. The policy may change as and when it is deemed necessary. New policies or changes to existing policies will become effective immediately following a brief announcement made by any means, including email, printed notices, or through newsgroups.

REGISTRAR
DOON UNIVERSITY
DEHRADUN (INDIA)

2. Email Account Use Policy

It is advised to use the university's e-mail services for formal university communication as well as for academic and other official reasons in an effort to boost the efficiency of the distribution of crucial information to all academics, staff, students, and the university's administration.
The transmission of messages and documents to the campus and wider communities, as well as to specific user groups and individuals, will be made easier with the use of email for official communications. Formal University communications are messages from the institution to its staff, faculty, and students.

Users might be informed that by using the email feature, they consent to the following rules:

1. The facilities should primarily be utilized for academic and professional reasons, with some personal use allowed.
2. The facility may be withdrawn if it is used for illicit or commercial activities, which is a clear breach of the university's IT policy. Unauthorized and illegal software copying or distribution, as well as sending unsolicited bulk e-mails, are only a few examples of illicit use as well as the creation of false, threatening, harassing, abusive, offensive, or vulgar words or images.
3. Make sure the recipient has email capabilities that allow him to accept such large attachments before sending large attachments to them.
4. Any email or attachment coming from an unknown or suspect source shouldn't be opened by the user. Even if it comes from a well-known source and contains an attachment that seems questionable or suspicious, the recipient should first authenticate its legitimacy with the sender. This is crucial from the user's computer's security perspective, as such messages may contain viruses that have the ability to harm the important data on your computer.
5. The user is responsible for maintaining a backup of their account's incoming and outgoing mail.
6. Because the account holder is solely responsible for any misuse of that email account, the user shouldn't share their email address with anybody else.
7. Any email account that another user unintentionally left open while using a shared computer should be immediately closed by the user who is currently using that computer without accessing its contents.
8. Users should refrain from intercepting or attempting to hack into other users' email accounts because doing so violates their privacy.
9. Impersonating someone else's email account will be treated seriously under the university's IT security policy.
10. The user should maintain the mail box's used space below the 80% use threshold.
11. In the end, it is each person's duty to keep their email account clean of contraventions of the university's email usage policy.

REGISTRAR
DOON UNIVERSITY
DEHRADUN (INDIA)

दून विश्वविद्यालय DOON UNIVERSITY
मोथरोवाला रोड, केदारपुर, पो०ओ० डिफेन्स कालोनी, देहरादून–248001 (उत्तराखण्ड) भारत
Mothrowala Road Kedarpur, P.O. Defence Colony, Dehradun-248001 (Uttarakhand) INDIA.

3. Social Media Policy

This policy offers guidelines for using social media by employees (who are permitted by competent authority). For the purposes of this policy, "social media" should be broadly construed to include What's App, message boards, chat rooms, electronic newsletters, online forums, social networking sites, and other websites and services that allow users to share information with others.

Rules

1. The usage of social media for business purposes by Doon University and personal purposes when mentioning Doon University are both subject to the aforementioned rules.
2. Social media platforms, blogs, and other forms of online content can occasionally attract press coverage or legal inquiries. The official University spokespersons should be contacted with these questions, not the staff members.
3. Employees should be conscious of the impact their activities may have on both their personal and Doon University's reputations when using social media in connection with the institution. Employees should be informed that The University may monitor material and information made available by employees through social media. The information that employees upload or publish may be publicly available for a long time. To submit content that is appropriate and not harmful to Doon University, its staff, or customers, employees should use their best judgment. Although not a comprehensive list, some particular instances of unacceptable social media behavior include posting comments, content, or photographs that are libelous, harassing, defamatory, pornographic, proprietary, or that could foster a hostile workplace environment.
4. No derogatory, offensive, embarrassing or abusive language should be used by employees in any comments or posts.
5. If workers come across a circumstance on social media that appears to be staff should politely exit the conversation if it becomes hostile and consult the human resources department for guidance.
6. Before referring to or posting photographs of current or former employees, members, vendors, or suppliers, employees should obtain the necessary authorization. Employees must also obtain the correct authorization before using another party's copyrights, copyrighted content, trademarks, service marks, or other intellectual property.
7. Social media usage shouldn't conflict with Doon University staff members' duties. Use of the university's computer systems must be for professional purposes.

REGISTRAR
DOON UNIVERSITY
DEHRADUN (INDIA)

8. A worker who engages in after-hours online activity that is against business policy or the law may face disciplinary action or termination.
9. If at all possible, staff should maintain their personal and Doon University-related social media profiles separate.
10. Any photograph that does not reflect their reputation as faculty or teachers (As they belong to a respected community).

4. Responsibilities of University IT & Computer Center(ITCC)

A. Maintenance of Computer Hardware & Peripherals

B. The ITCC is in charge of maintaining all university-owned computer systems and peripherals that are covered by a warranty or a yearly maintenance agreement and for which this Cell has been given formal authority.

C. Receiving Complaints

(i) If any particular computer system is producing network-related issues, ITCC may get complaints from INTERNET UNIT.

(ii) If any of the computer systems or peripherals that are being serviced by ITCC are experiencing issues, the users may contact the centre with concerns.

(iii) The authorised individual in the ITCC gets complaints from users and the Internet Unit of various computer systems, and they work along with the service engineers of the relevant brands of computer systems to find a reasonable solution.

Scope of ITCC Services

D. Only issues with the operating system or any other application software that the university has legitimately purchased and that the company has loaded will fall under the ITCC's purview.

E. **Installation of Un-authorized Software**

The user's computer systems should not be encouraged by ITCC or its service technicians to run any unlawful software. They must rigorously avoid complying with such solicitations.

F. **Reporting IT Policy Violation Incidents**

Applications that interfere with network operations or with the IT policies of the university should be reported to the INTERNET UNIT and university administrators if they are discovered by ITCC or its service engineers.

G. **Reporting occurrences involving network operations**

The Internet Unit will notify the Computer Center when the network port of any specific computer system is disabled owing to a virus or other associated behavior that is impairing network performance. In order for the port to be turned on by the Internet Unit once ITCC or service engineers have taken the appropriate corrective action, they must be informed of the same.

REGISTRAR
DOON UNIVERSITY
DEHRADUN (INDIA)

H. Rebuilding the Computer System

Care should be made to provide the same hostname, IP address, network Mask, and gateway when the service engineers reformat the computer systems and reinstall OS and other application software. Additionally, all updates and the most recent service pack should be correctly installed after the OS. When it comes to antivirus software, service technicians should make sure to get the most recent engine and pattern files from the internet as well.

Additionally, a backup of just the data files should be made before formatting the hard drive. Software files from the corrupted hard disc dump should never be used to restore the formatting hard disc.

I. Internet unit coordination

When there is a question as to whether a specific issue on a computer linked to the network is due to the network, the software that has been installed, or faulty hardware, a computer center/service engineer may collaborate with the employees from the internet unit to remedy the issue. The user shouldn't be allowed to handle this task alone.

5. Guidelines for Desktop Users

These rules apply to all DU Network User Community participants and University network users.

University IT Policy has developed suggestions to improve desktop security in response to the rise in hacker activity on campus.

The following suggestions comprise:

1. The most recent antivirus software should be installed on every desktop computer. The configuration that schedules regular updates of virus definitions from the main server should also be kept in place.
2. All operating system updates and patches must be installed on a desktop computer. Patches and operating system upgrades should also be applied continuously, on a regular basis. The frequency will strike a balance between the necessity for security and the impact on production (while patches are installed). For each machine, we suggest a weekly cycle. Security guidelines must to be established at the server level and implemented to desktop computers wherever practical.
3. All Windows workstations (and Macintosh desktops running OS X or later) ought to have an administrator account that isn't used for routine login. Change the administrator account's default login information.
4. The password need to be challenging to guess. Password is defined as:
   (i). having a minimum of 6 to 8 characters;
   (ii). requiring punctuation, such as! $% & *,.? + - =, etc. must begin and end with letters
   (iii). cannot contain the symbols # @'" '
   (iv) must be brand-new and unused
   (vi). one should refrain from using his name, the names of his wife or children, the name of his department, the number of your room or house, etc. which are easy to guess.
   (vii). passwords should be changed periodically and also when suspected that it is known to others.

REGISTRAR
DOON UNIVERSITY
DEHRADUN (INDIA)

(viii). Never use 'NOPASS' as your password
(ix). Do not leave password blank and make it a point to change default passwords given by the software at the time of installation

5. The user login password should adhere to the criteria mentioned above.
6. You ought to disable the guest account.
7. The built-in firewall on new Windows workstations needs to be turned on.
8. If the OS does not come with an in-built firewall, all users should think about using a personal firewall, which typically comes with the anti-virus software.
9. The hacked computer systems should have all of their software completely reinstalled.
10. Unless absolutely necessary, avoid installing Microsoft IIS and don't activate any of its features.
11. In general, open up services as needed, starting from the position of security that is the most secure (i.e., no sharing, no guest access, etc.). In addition to the above suggestions, INTERNET UNIT recommends a regular backup strategy.
12. The port will be closed if a machine is compromised, according to INTERNET UNIT. As long as the computer is fixed in accordance with the rules, this will isolate it. The port will then be turned back on at that point.
13. Standard filters can be applied at the subnet level for departments or schools with their own subnets and administrators. If a department or school has its own servers, technical staff from the INTERNET UNIT can request to examine the servers for vulnerabilities.

It should be remembered that even with all the steps outlined above, a virus infection or hacker compromise is still a possibility. Regular data backups (daily and/or weekly) will help to decrease the impact of losing a machine.

6. Video Surveillance Policy

1.0 The surveillance system

1.1 The system includes public information signs, monitors, multiplexers, digital recorders, fixed position cameras, pan, tilt, and zoom cameras, and SAN/NAS storage.

1.2 Cameras will be located at strategic points on the campus, principally at the entrance and exit point of sites and buildings. No camera will be hidden from view and all will be prevented from focusing on the frontages or rear areas of private accommodation.

1.3 To alert staff, students, visitors, and members of the public that a CCTV/IP Cemera system is in use, signs will be conspicuously displayed at key locations as well as at the entrance and exit points of the campus.

REGISTRAR
DOON UNIVERSITY
DEHRADUN (INDIA)

1.4 Even though every effort has been taken to assure the system's maximum performance, it is impossible to guarantee that it will catch every occurrence that occurs within the coverage area.

2.0 Purpose of the system

- The institution installed the system with the major goals of lowering the threat of crime generally, securing the university's property, and assisting in ensuring the safety of all staff, students, and visitors while respecting their right to privacy.
- These goals will be accomplished by keeping an eye on the system to
- discourage those with criminal intent;
- aid in the prevention and detection of crime;
- facilitate the identification, apprehension, and prosecution of offenders in relation to crime and public order;
- Facilitate the identification of any activities or events that might warrant taking disciplinary action against staff or students and help in providing evidence to managers and/or a member of staff or the appropriate authorities.
- The technology will not be used in the event of security personnel to provide management information regarding employee compliance with employment contracts:
  (a) To offer captured photographs for the internet.
  (b) To record sound in a manner inconsistent with the covert recording policy.
  (c)When making an automatic choice

3.0 Covert recording

- On the written request or authorization of the Senior Officer, Registrar, and when it has been determined by the Head of Security and Facilities Services and the Data Protection Officer, covert cameras may be deployed in the following situations.

  (a) Because telling the person(s) in question that a recording was being made would substantially undermine the recording's purpose; and

  (b) that there is a solid basis for suspicion that illegal or unauthorised action is occurring or about to occur.

  - Any such covert processing will only be done for a brief amount of time that is reasonable given the recording's goals and will only be relevant to the particular suspected unauthorised behaviour.

  - The decision to employ covert recording will be clearly documented, outlining who made the decision and how it was reached.The Security Control Room

REGISTRAR
DOON UNIVERSITY
DEHRADUN (INDIA)

- The Security Control Room, sometimes known as "the control room," will monitor and record all images taken by the system around-the-clock throughout the entire year. The control room's outside does not have a view of the monitors.

- At no point will unauthorised entry be allowed to the Control Room. Access will only be granted to authorised senior management, police officers, duty controllers, and other individuals with legal entry rights.

- Access to the Control Room may be granted to staff, students, and visitors on a case-by-case basis and only after receiving written consent from the Registrar. Access may be provided to someone having a valid purpose to enter the Control Room in an emergency and when it is not reasonably practicable to gain previous authorization.
- Staff must be certain of a visitor's identification and that they have the necessary authorization before providing them admission to the Control Room. All visitors must fill up and sign a visitors' log that includes information about them, the department or organisation they represent, who gave them permission to visit, when they entered and left the centre, and their name. A comparable log will be kept of the security control room staff members on duty and any guests who have been given emergency access.

4. Security control room administration

A copy of the Procedures Manual, which is accessible for examination by prior arrangement with a request indicating the reasons, contains specifics of the administrative procedures that apply to the Control Room.

- The Prevailing Data Protection Act's rules apply to images of identifiable live people, and the Control Room Supervisor is in charge of ensuring day-to-day compliance. The processes outlined in the Procedures Manual and this policy will be strictly followed when handling all recordings.

5. Staff

The sensitivity of handling CCTV/IP Camera images and recordings will be made clear to every employee working in the security control room. The control room supervisor will see to it that every member of staff is properly informed and taught regarding the operational and administrative ramifications of using CCTV/IP cameras.

6. Recording

Digital video recorders in time-lapse mode are used to create digital recordings. Real-time incident recording is possible.

REGISTRAR
DOON UNIVERSITY
DEHRADUN (INDIA)

Images are often automatically overwritten and the Log updated after fifteen days have passed since the date of recording. A hard drive will be erased before disposal once it has served its purpose, and the Log will be updated as a result.

Up until disposal and destruction, all hard drives and recorders shall remain the property of the institution.

7. Access to images

According to the Procedures Manual, every access to an image shall be noted in the Access Log.

Only the staff members who need access to the photos in order for the system to function properly will be granted access.

(1) Access to images by third parties

- Only the authorities listed below may disclose recorded material to third parties in strict conformity with the system's objectives:
- Law enforcement agencies when the photos captured might help with a criminal investigation and/or the suppression of terrorism and disturbance
- Prosecution authorities
- Appropriate legal counsel
- The media in situations where enlisting the help of the public is necessary to identify a victim of crime or a perpetrator of a crime
- Individuals whose photographs have been captured and stored, unless disclosing them to them would jeopardize criminal investigations or criminal procedures.
- Emergency services in connection with an accident inquiry.

(2) Subject's ability to view photos

7.2.1. If digital CCTV/IP camera photos of a person can be recognized, they are considered personal data and are protected by the Data Protection Act. Anyone who suspects that they have been videotaped by \sC.C.T.V. /IP Cemera is entitled to ask for a copy of the data, subject to exemptions specified in the Act. They are not entitled to immediate access.

7.2.2 The Data Protection Officer must receive a written request from a person whose image has been captured and stored if they want access to the data. Subject Access Request Forms can be obtained from the Security Office between the hours of 1020 and 1400 and 1430 to 1800 on weekdays (excluding the second and fourth Saturday) or from the Data Protection Officer at the Records Office during the same hours, unless the university is officially closed.

REGISTRAR
DOON UNIVERSITY
DEHRADUN (INDIA)

7.2.3 The Data Protection Officer will then make arrangements for the applicant to receive

Copy of the data. The applicant is not permitted to request a copy of the data from another employee or to request that another employee show them the data. The university's data protection officer must be contacted for all interactions. After receiving the needed fee and information, a response will be sent immediately and, in any case, inside of forty days.

7.2.2 Under the Data Protection Act, the Data Protection Officer has the authority to deny a request for a copy of the data, especially if doing so could jeopardize efforts to prevent or detect crime, apprehend offenders, or prosecute them.

7.2.3 The Security Control room Supervisor or the Data Protection Officer shall be contacted regarding each of these requests.

7.2.4 If a decision is made to deny a data subject access request, the decision will be thoroughly documented, and the data subject will be notified in writing and given the justifications.

8. Request to prevent processing

8.1 A person has the right to ask for the prevention of processing when it is likely to result in significant and unjustified harm or distress for them or another person.
8.2 The Security Control Room Supervisor or the Data Protection Officer should be contacted with any such requests first. They will respond in writing, outlining their decision, within 21 days of receiving the request. Both the request and the answer will be kept on file.

9.0 Complaints

9.1.1. It is acknowledged that students, faculty, staff, and others may have issues with the way the system is run.
9.1.2. Any grievance should be brought up with the security control room supervisor right away. The complainant may use the Universities Centralized Complaints Procedure by receiving and completing a University Complaints Form and a copy of the procedure if, after following the procedures outlined, the issue is still unresolved.
9.1.3. The Security Office and the Registrar's Office both sell complaint forms. The Data Protection Officer can be contacted with questions or concerns regarding the requirements of the current Data Protection Act.
9.1.4These rights do not change the rights that University members or others currently have under any applicable grievance or disciplinary procedures.

REGISTRAR
DOON UNIVERSITY
DEHRADUN (INDIA)

दून विश्वविद्यालय
मोथरोवाला रोड, केदारपुर, पो०ओ० डिफेन्स कालोनी,
देहरादून–248001(उत्तराखण्ड) भारत

DOON UNIVERSITY
Mothrowala Road Kedarpur, P.O. Defence Colony,
Dehradun-248001 (Uttarakhand) INDIA.

DECELARATION

I,----------, Employee ID/Enrollment No:,----------, hereby affirm that I will adhere by the aforementioned guidelines as an employee or student at Doon University. I acknowledge that any action I do that could be construed as a breach of this policy will be punished in accordance with rule #13.

Date:_____ **Signatur _____**

REGISTRAR
DOON UNIVERSITY
DEHRADUN (INDIA)