University of Petroleum & Energy Studies: Acceptable IT Use policy v3.0, 2013

1/23/2013
University of Petroleum & Energy Studies
Central IT Services

DISCLAIMER

UPES reserves the right, without notice, to limit or restrict any individual's use, and to inspect, copy, remove, or otherwise alter any data, file, or system resource which may undermine the authorized use of any computing facility or which is used in violation of UPES rules or policies.

UPES also reserves the right periodically to examine any system and other usage and account activity history as necessary to protect its computing facilities.
While UPES will make all reasonable efforts to ensure privacy and confidentiality of user data and availability of service to users, UPES disclaims any responsibility for loss of data or interference with files resulting from its efforts to maintain the privacy and security of those computing facilities or from system malfunction or any other cause.

UPES also reserves the right to amend these policies at any time without prior notice and to take action as necessary or appropriate to comply with applicable laws.

Contents

Acceptable IT Use 5
1.0 Computing Resources 5
1.1 Applicability 5
1.2 Rights & Responsibilities 5
1.3 General Guidelines 5
1.4 Security & Privacy 6
1.5 Supported Software 7
1.6 Prohibited downloads 8
1.7 Enforcement 8
2.0 E-Mail policy 9
2.1 E-mail to students policy 9
2.1.3 Use of student accounts 10
2.1.4 Forwarding of E-mail 10
2.2 E-mail address creation, disposal and retention policy 10
2.2.1 Purpose 10
2.2.2 Employee Accounts 10
2.2.3 eMail Retention and Recovering Deleted Email via Backup Media 10
2.3 E-mail list policy 11
2.3.1 Overview 11
2.3.3 Scope 11
2.3.4 Policy 11
3.0 Commercial Use Policy 12
4.0 Web Pages Policy 12
5.0 Commercial Pages Policy 13
6.0 External Links Policy 13
7.0 Excessive or Disruptive Use Policy 13
8.0 Network Infrastructure/Routing Policy 13
9.0 Wireless Policy 13
10.0 Virtual Private Network (VPN) Policy 14

11.0 Encryption policy 14
Definitions 14
11.1 Purpose 14
13.0 Notebook security 16
13.1 Purpose 16
13.2 Safety and Security Guidelines 16
14.0 Password Policy 18
Definitions 18
14.1 Overview 18
14.2. Purpose 18
14.3. Scope 18
14.4. Policy 18
14.4.1. General 18
14.4.2. Application Development Standards 19
14.4.3. Use of Passwords and Passphrases for Remote Access Users 19
14.5 Enforcement 19
15.0 Guidelines for Foreign students 19
15.1 Using UPESNET 20
15.1.1 Use DHCP to obtain an IP address automatically 20
15.1.2 Using wireless 20

Acceptable IT Use

1.0 Computing Resources

As part of its educational mission, the University of Petroleum & Energy Studies (UPES) acquires, develops, and maintains computers, computer systems and networks. These computing resources are intended for University-related purposes, including direct and indirect support of the University's instruction, research and service missions; University administrative functions; student and campus life activities; and for free exchange of ideas within the University community and wider local, national, and world communities.

1.1 Applicability

i. This policy applies to all users of University computing resources, whether affiliated with the University, and for use of those resources, whether on campus or other remote locations.

ii. “Users” are defined as anyone who uses University systems or networks including employees, students, parents, vendors, contractors, support personnel etc.

This policy also governs specific computers, computer systems or networks provided or operated by specific units of the University. This policy may be modified as deemed appropriate by the University from time to time as posted on the University's Intranet.

1.2 Rights & Responsibilities

The right of academic freedom and freedom of expression applies to the users of University computing resources. So do the responsibilities and limitations associated with those rights. While the University’s campus and computing environment will be open to free expression of ideas, including unpopular points of view, the use of its computing resources, like the use of other University-provided resources and activities, is subject to the requirements of legal and ethical behavior. Thus, legitimate use of a computer, computer system or network does not extend to whatever is technically possible.

1.3 General Guidelines

i. Users of University computing resources shall comply with applicable national laws, applicable State Laws, University rules and policies, and the terms of applicable contracts including software licenses while using University computing resources. Examples of applicable laws, rules and policies include the laws of privacy, copyright, trademark, obscenity and child pornography; the IT Act 2000, which prohibits "hacking," "cracking" and similar activities.

ii. Users who engage in electronic communications with persons in other states or countries or on other systems or networks may also be subject to the laws of those jurisdictions and the rules and policies of those other systems and networks. For further clarifications, users should contact the Chief Information Officer or the Vice Chancellor, UPES for more information.

iii. Users will be required to obtain necessary authorizations before using University computing resources. Any hardware/physical asset issued to a user must not be tampered with or given for repair/replacement outside of University authorized vendors. If emergency off-campus repairs are warranted, prior approval should be taken from the IT Manager at the users base location or from

the Corporate office in Delhi. Users will also be responsible for any activity originating from their accounts which they are reasonably expected to control.

iv. For any loss/damage of issued assets, the University will bear losses up to Rs. 5,000/- (rupees five thousand only) for the duration of the users service. A record will be kept of such losses and if the above limit is exceeded, appropriate disciplinary enforcement shall apply. Any insurance claim amounts that are received will offset the negative balance to the extent of Rs. 5,000/- (rupees five thousand.)

v. Accounts and passwords should not, under any circumstances, be used by persons other than those to whom they have been assigned by the systems administrator. In cases when unauthorized use of accounts or resources is detected or suspected, the account owner should change the password and report the incident to the appropriate systems administrator, and/or Dean, Director, or Department Head.

vi. While no set bandwidth, disk space, CPU time, or other limit are applicable to uses of University computing resources, the users are required to limit or refrain from specific uses if, in the opinion of the Chief Information Officer, such use interferes with the efficient operations of the system.

vii. Users should not state or imply that they speak on behalf of the University or use University trademarks and logos without authorization to do so. Authorization to use University trademarks and logos on University computing resources may be granted only by the Office of Corporate Relations. The use of appropriate disclaimers is encouraged.

viii. Users shall not use computing resources to gain unauthorized access to remote computers or to impair or damage the operations of UPES computers or networks, terminals or peripherals. This includes blocking communication lines, intercepting or sniffing communications, and running, installing or sharing virus programs.

ix. Users should not bring personal mass storage devices into the University network and should not use such devices to store official data for backup purposes. Designated backup locations and procedures should be used for this purpose (Drive X: provided to all campus users). Deliberate attempts to circumvent data protection or other security measures will be dealt with seriously. All data that is deemed important / critical from an organization perspective should be copied on the users X: Drive at the end of each working day. This includes but is not limited to informational lists, emails, presentations, documents, internal memos, and external communication. Following this procedure ensures that there is a retrievable copy of the data should any unforeseen eventuality occur on the users machine. Data on Drive X: is regularly backed up on central systems.

1.4 Security & Privacy

i. While the University employs various measures to protect the security of its computing resources and its user's accounts, it cannot guarantee security and confidentiality. Users should therefore engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords and changing them regularly as well as storing critical data in University defined storage locations.

ii. Users should also be aware that their uses of University computing resources are not completely private. While the University does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the University's computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns

and other such activities that are necessary for the provision of service. The University may also specifically monitor the activity and accounts of individual users of University computing resources, including individual login sessions and the content of individual communications, without notice, when:

- The user has voluntarily made them accessible to the public, as by posting to a newsgroup or a Web page;
- It reasonably appears necessary to do so to protect the integrity, security, or functionality of University or other computing resources or to protect the University from liability;
- There is reasonable cause to believe that the user has violated or is violating this policy;
- An account appears to be engaged in unusual or unusually excessive activity; or it is otherwise required or permitted by law.

iii. Any such monitoring of communications, other than what is made accessible by the user, required by law, or necessary to respond to perceived emergency situations, shall be authorized in advance by the appropriate Dean / Director or the Chief Information Officer. The University, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate University authorities or law enforcement agencies and may use those results in appropriate University disciplinary proceedings. Communications made through University computing resources will also be generally subject to the Indian IT Act, 2000 to the same extent as they would be if made on paper.

iv. Visitors to UPES Web sites who are not currently UPES students, faculty or staff should refer to the University's Disclaimer and Terms of Use for privacy information.

1.5 Supported Software

i. Unless otherwise specified, the following is a list of software approved by the University and supported by central IT. These applications will be installed and maintained for all security patches and updates on computers owned by the University:
   a. Base Operating System (Microsoft Windows)
   b. Office Automation Suite (Microsoft Office)
   c. Acrobat Reader and generator (if required)
   d. File compression utility
   e. Email client
   f. Web Browser (Microsoft Internet Explorer / Mozilla Firefox or Google Chrome)
   g. Anti virus software (Symantec Endpoint Protection)
   h. ORACLE client (if required)
   i. Licensed Domain specific software on lab computers
   j. Rich media players (VLC or Quicktime)
   k. E-book readers (Microsoft, Kindle or other standards compliant reader)

ii. Apart from the above set of software, any applications that are installed by the user are done at their own risk. Central IT assumes no responsibility for the correct functioning of the user's PC or safety of their data should such applications cause damage to files / data. Users are advised to take clearance from the CIO before installing applications on their systems.

1.6 Prohibited downloads

The following downloads are specifically not allowed on computers unless approved in writing by Central IT:

a) Any peer to peer file sharing application: Such applications may be used to utilize bandwidth inappropriately. Further, these applications contain third-party applications – called adware or spyware, that collect information about a user's Web surfing habits, change system settings, or place unwanted advertising on the local computer.

b) Any third party personal antivirus or firewall: Since adequate security has already been provided for on all machines via pre-defined firewall rules, third party firewalls may interfere with these rules thus endangering the network.

c) Any third-party screen saver or wallpaper: This is to prevent images that might be deemed offensive by some users from being displayed on monitors. Users should use the default screen savers available on their local machines.

d) Hacking tools of any sort: The use of any such tools on University machines is strictly prohibited.

e) Games & Movie trailers or previews: These provide no productive academic benefit and have a tendency to affect productivity, and hence are not allowed on University machines. Users who use their own local machines / University provided portables on which to work are exempt from this policy. For this purpose, games could be in any form – executables or flash based games downloaded from the Internet.

1.7 Enforcement

i. Users found violating this policy may be denied access to University computing resources and may be subject to other penalties and disciplinary action, including possible expulsion or dismissal.

ii. Alleged violations will be handled through the University disciplinary procedures applicable to the user.

iii. The University may suspend, block or restrict access to an account, independent of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of University or other computing resources or to protect the University from liability.

iv. The University may also refer suspected violations of applicable law to appropriate law enforcement agencies.

v. General enforcement applicable If a user is found in violation of the above, will be:

- First time offence – Account suspension for one week (7 working days) unless countermanded in writing by the Administrative Head of the location as applicable to the user.
- Second time offence – Account suspension for two weeks (14 working days) subject to the above provision.
- Repeat offences – information to the applicable disciplinary process for suitable action

2.0 E-Mail policy

i. For purposes of this document, e-mail includes point-to-point messages, postings to newsgroups and listserves and any electronic messaging involving computers and computer networks. Organizational e-mail accounts, including those used by student organizations, are held to the same standards as those for individual use by members of the University community. E-mails are also generally subject to the IT Act, 2000 to the same extent as they are on paper.

ii. Examples of Inappropriate Uses of E-mail:

a. The following uses of e-mail by individuals or organizations are considered inappropriate and unacceptable at the University of Petroleum & Energy Studies. In general, e-mail shall not be used for the initiation or re-transmission of:

- Chain mail that misuses or disrupts resources - E-mail sent repeatedly from user to user, with requests to send to others;
- Harassing or hate-mail - Any threatening or abusive e-mail sent to individuals or organizations that violates University rules and regulations;
- Virus hoaxes;
- Spamming or e-mail bombing attacks - Intentional e-mail transmissions that disrupt normal e-mail service;
- Junk mail - Unsolicited e-mail that is not related to University business and is sent without a reasonable expectation that the recipient would welcome receiving it; and
- False identification - Any actions that defraud another or misrepresent or fail to accurately identify the sender.

b. The University may add more such inappropriate uses from time to time as deemed necessary.

2.1 E-mail to students policy

The University of Petroleum & Energy Studies (UPES) utilizes e-mail as one of the official means of communication with students to keep them informed of important information such as financial aid and billing data; college deadlines, events and updates; and important campus news. Each student is issued an official e-mail account for use while he or she is enrolled.

2.1.1 General Guidelines

E-mail is an appropriate and preferred method for official communication by UPES with students unless otherwise prohibited by law. The University reserves the right to send official communication to students by e-mail with the assumption that students will receive, read and, if necessary, act in a timely manner based upon these e-mails.

2.1.2 Assignment of student accounts

Upon confirmation of admission to UPES, a University e-mail account is automatically created for each student in the form of initialslastname@stu.upes.ac.in or as otherwise determined by IT Services. Official e-mail accounts are maintained by IT Services and will be published online and in the student directory. This e-mail address remains with the student throughout their academic career at UPES as well as afterwards should the student choose to use it.

2.1.3 Use of student accounts

i. It is the responsibility of students to access and maintain these accounts in accordance with other University electronic communication policies including, but not limited to, the Acceptable Use Policy.

ii. Students are expected to check their email on a frequent and consistent basis. Students must make sure that there is sufficient space in their accounts to allow for e-mail to be delivered and have the responsibility to recognize that certain e-mails may be time sensitive. Students will not be held responsible for an interruption in their ability to access a message because of system problems that prevent timely delivery of, or access to, messages. These include scheduled and unscheduled outages of the system.

2.1.4 Forwarding of E-mail

Students who choose to have their email forwarded to an unofficial e-mail address will do so at their own risk. UPES is not responsible for any e-mail beyond delivery to UPES official accounts. Students are however responsible for official e-mail as outlined above.

2.2 E-mail address creation, disposal and retention policy

2.2.1 Purpose

i. This e-mail Policy is intended to help faculty, staff, and students understand when and how their accounts are created and determine what information sent or received by email should be retained and for how long.

ii. The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via electronic mail or instant messaging technologies.

iii. All Faculty, Staff, and Students should familiarize themselves with this eMail policy.

iv. Questions about the proper retention of a specific piece of information should be addressed to the users administrative reporting officer.

v. Questions about these guidelines should be addressed to the eMail Administrator or Chief Information Officer.

2.2.2 Employee Accounts

i. Faculty/Staff accounts are created when new employees are entered into the HR system. Their accounts will be available for use the day after they are entered into HR. An individual can contact the IT Services helpdesk to obtain their user name.

ii. Deactivation - Faculty/Staff accounts will be deactivated when they are changed to an "inactive" status in HR and have no other role in SAP (e.g. also not a student).

iii. Student accounts will be deactivated from the system when their status in SAP changes to inactive – either by reason of graduation or withdrawal from the University.

2.2.3 eMail Retention and Recovering Deleted Email via Backup Media

All University email information is retained for 1 month; after that time backup media will be over-written. UPES maintains backups from the email server and once a month a set of disks is taken out of the rotation and moved offsite.

2.2.4 Encrypted Communications

i. UPES encrypted communications should be stored in the following manner:
   a. The encryption standard used should be 3DES / PGP secured using at least 128 bit encryption.
   b. The decryption keys should be available with the user's supervisor to be used in the event of the data being needed in the absence of the user.
   c. Any use of the decryption key should be with the explicit permission of the Dean / Director or Head of Department.

ii. In general, information should be stored in a decrypted format – unless deemed sensitive by the University.

2.3 E-mail list policy

2.3.1 Overview

Management of e-mail lists is an important service to assist University constituencies communication efforts. As such, all University IT Services users are responsible for understanding the types of lists available and for following defined processes for requesting e-mail lists.

2.3.2 Purpose

The purpose of this policy is to establish standards for E-Mail Lists.

2.3.3 Scope

The scope of this policy includes all IT Services personnel.

2.3.4 Policy

- A Request must be created for new e-mail list requests in the Helpdesk, regardless of first point of contact.
- A Technical Support Specialist shall be assigned to work with user requesting the e-mail list to determine specifications and, if the request is approved, provide training once the list is established
- If the list is for one area or the requestor provides a specific set of e-mail addresses, the request will be approved; however, if the request crosses functional/departmental areas or requests "all" users the request must be routed through the appropriate office.
- Lists including on-campus e-mail addresses only and does not require the functionality of a listserv will use a distribution list that is maintained in the Global Address Book.
- Lists including off-campus e-mail addresses or a combination of on and off-campus addresses will use third party applications.
- All lists will have a user as a "list administrator" assigned; the administrator is the person from the area/group requesting the list
- Both types of e-mail lists are maintained by the administrator of the list, not by IT Services
- Both types of e-mail lists have a limit of 5,000 e-mail addresses per list

3.0 Commercial Use Policy

i. Computing resources are not to be used for personal commercial purposes or for personal financial or other gain.

ii. Occasional personal use of University computing resources for other purposes may be permitted provided it does not lead to excessive use of those resources, does not interfere with the performance of the user's job or other University responsibilities, and is otherwise in compliance with this policy.

iii. Further limits may be imposed upon personal use in accordance with normal supervisory procedures concerning the use of University equipment.

4.0 Web Pages Policy

i. Official University pages (including colleges, departments, bureaus, centers, institutes, etc.) represent the University and are intended for the official business functions of the University.

ii. Each official home page must use an address that ends in ".upes.ac.in" and be registered with the University's Web administrator who will then include it as a link from the UPES Website or intranet.

iii. The following information must be readily accessible on the main page:

- The name of the unit or group represented by the page;
- Contact details of the person(s) responsible for maintaining the page content;
- Date of last revision;
- The unit logo (if separate from the University logo); and
- An active link to the UPES home page.

iv. Personal web space is provided for University network account holders at: http://lms.ddn.upes.ac.in/mymoodle User pages represent the individual in his or her primary role as a UPES user. Incidental personal information on user pages is deemed acceptable so long as it does not interfere with the function or desired presentation of the unit, cause disruption of normal service, incur significant cost to the University or result in excessive use of resources.

v. Faculty and staff who wish to publish substantial personal information not related to their University functions should use an Internet service provider rather than using University Web resources.

vi. User posting on official University forums / Social media accounts must be done in a personal capacity and must not contain / disclose any confidential/proprietary information. They should not be derogatory, inflammatory, or insulting to any member of the University community or to any other user, or based on fallacious facts. It should be noted that such postings are the user's personal opinion and do not represent the University's views in any way. It is the University's prerogative to suitably amend/remove posts that do not conform to the above as well as initiate disciplinary action against the poster- including and up to termination of services.

5.0 Commercial Pages Policy

i. Using UPES Web pages for personal gain is forbidden. Any private commercial use of UPES Web pages must be pre-approved pursuant to existing University policies and procedures regarding outside employment activities.

ii. All UPES units that accept payment electronically via the Internet are required to process all such transactions through the approved payment gateway.

6.0 External Links Policy

UPES accepts no responsibility for the content of pages or graphics that are linked from UPES pages. However, Web page authors should consider that such links, even when clearly labeled, can be misinterpreted as being associated with the University. Links to pages where users have a personal monetary interest are likely to violate policies regarding advertising and commercial use and should be avoided.

7.0 Excessive or Disruptive Use Policy

Excessive or disruptive use of University resources in the viewing or publishing of Web pages is not permitted. Colleges, Departments, or Centres owning or administering the resources involved will determine whether specific usage is considered normal, excessive or disruptive.

8.0 Network Infrastructure/Routing Policy

i. Users must not attempt to implement their own network infrastructure including, but is not limited to basic network devices such as hubs, switches, routers, network firewalls, and wireless access points. Users must not offer alternate methods of access to UPES IT resources such as modems and virtual private networks (VPNs).

ii. Users must not offer network infrastructure services such as DHCP and DNS. Exceptions to this policy must be coordinated with the local network administrator with prior approval from the Chief Information Officer.

9.0 Wireless Policy

i. For the purposes of this document, we refer only to wireless transmission using radio frequency (RF). As wireless is a shared media and easily intercepted by a third party, wireless users are encouraged to use some type of encryption. Use of the WPA2-AES or WPA2-TKIP encryption protocols is suggested to encrypt wireless communication.

ii. Improperly configured wireless access points (WAPs) might cause denial of service to legitimate wireless users and can also be used to subvert security. Wireless access points must be authorized by the Systems Administrator.

10.0 Virtual Private Network (VPN) Policy

i. A VPN provides secure encrypted access between a client and the VPN server. They are most commonly used to secure access to a trusted network from remote, untrusted networks.
ii. VPN servers must be authorized by the Chief Information Officer.

11.0 Encryption policy

Definitions

Proprietary Encryption: An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.

Symmetric Cryptosystem: A method of encryption in which the same key is used for both encryption and decryption of the data.

Asymmetric Cryptosystem: A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

11.1 Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have been proven to work effectively.

11.2 Scope

This policy applies to all UPES users and affiliates.

11.3 Policy

University faculty and staff are encouraged to encrypt files, documents, and messages containing sensitive or confidential University information for protection against unauthorized disclosure while in transit.

However, any encryption performed on University systems must use proven standard algorithms and such encryption must permit properly designated University officials, when required and authorized to decrypt the information.

Proven, standard algorithms should be used as the basis for encryption technologies. Examples of standard encryption tools include:

- Pretty Good Privacy (PGP), which uses a combination of IDEA and RSA or Diffie-Hillman

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by Information Technology Services.

11.4 Enforcement

Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

12.0 Network traffic priorities

IT Services uses a network utility to control and prioritize the types of traffic on the University's Internet connection.

This network utility can...

- classify network traffic into categories based on application, protocol, subnet, Internet location, and other criteria
- provide statistical measurements on the peak and average bandwidth being requested by the above categories
- apply policy based allocation of bandwidth and traffic to protect core University applications and pace less urgent traffic, and
- provide reports based on the statistics and performance standards.

Currently, IT Services is limiting the bandwidth of a number of file sharing services including BitTorrent.

13.0 Notebook security

13.1 Purpose

This procedure describes security measures required to protect portable information assets (and the information that resides on these devices) such as notebook or tablet computers, personal digital assistants (PDA's), CDs, flash drives, DVDs, pagers, cell phones or other similar equipment from theft, loss or damage. Each user must follow the requirements for protecting University information, as set forth in UPES Information Sensitivity Policy (restricted to campus).

13.2 Safety and Security Guidelines

The practices listed below do not cover all potential risks, but will significantly minimize the likelihood of theft, loss or damage to University equipment and information. They may apply to one type of device and not another; the user is responsible for applying the measures appropriate to the device.

- If you travel with a notebook, make sure that you have the notebook case, including all its contents, over your shoulder before you leave the plane, taxi or train. When passing through a security checkpoint, keep your eyes on the device and pick it up as soon as possible.
- Make a record of the make and model of the notebook and any serial or company identification number on the equipment and store the record in a separate safe place.
- If you must leave a notebook or other device in a vehicle, put it out of sight and lock the vehicle or lock it in the trunk. Do not leave equipment in the vehicle at all in very cold or very hot weather, as extreme temperatures may cause damage.
- In an office or work area shared with others, or in an area accessible by the public, either secure the notebook, or other device, or keep it with you at all times. Never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the notebook and any other sensitive material in a locked drawer or cabinet.
- Back up your data frequently and store the files in a safe location separate from the notebook or other device.
- Encrypt or password-protect each file containing confidential and/or sensitive University information. Make passwords difficult to crack. A mixture of special characters, numbers, and upper and lower case letters is considered the most secure — but only if passwords are not stored on the hard disk. If your notebook comes with biometrics software (such as fingerprint imaging) configure the notebook to use it.
- Sensitive and/or Critical information includes, but is not limited to:
    - All information identifiable to an individual (including students, staff, faculty, trustees, donors, and alumni) including but not limited to dates of birth, personal contact information student education records, medical information, benefits information, compensation, loans, financial aid data, alumni information, donor information, and faculty and staff evaluations.
    - The University's proprietary information including but not limited to intellectual research findings, intellectual property, financial data, and donor and funding sources.
    - Information, the disclosure of which is regulated by government

- Restrict plug and play. Plug and Play is convenient, but can sometimes be dangerous: if someone connects a USB flash drive, MP3 player or external hard disk drive to a notebook, it is recognized automatically — and it is then easy to start exporting data.
- If your notebook is lost or stolen file an FIR with the Police and report the device's serial number as lost or stolen to the IT Services Help Desk.

14.0 Password Policy

Definitions

Application Administration Account
Any account that is for the administration of an application (e.g., Oracle database administrator, SAP administrator).

14.1 Overview

Passwords are a critical aspect of computer security forming the front line of protection for user accounts. A poorly chosen password can result in the compromise of the entire University's network. As such, all University students and users (including contractors and vendors with access to University systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

14.2. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

14.3. Scope

The scope of this policy includes all users who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any University facility, has access to the University network, or stores any non-public University information.

14.4. Policy

14.4.1. General

1. All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a semi-annual basis.
2. All production system-level passwords must be part of the IT Services administered global password management database.
3. All user-level passwords (e.g., email, web, desktop computer, etc.) must have
    1. Maximum password age of 180 days
    2. Minimum password age of 2 days
    3. Exhibit complexity by
        1. Not containing all or part of the user's account name
        2. Contain characters from three of the following four categories:
            1. Uppercase characters (A through Z)
            2. Lowercase characters (a through z)
            3. Base 10 digits (0 through 9)
            4. Non-alphabetic characters (for example, !, $, #, %)
    4. Maintain a password history of 2 passwords and not allow reuse
    5. Must be a minimum of 8 characters
    6. Be locked out if more than 5 unsuccessful attempted logons
4. Applications will automatically log-offs after a predetermined period of inactivity; username and password will be required for re-authentication.

5. User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
6. Username and password combinations must not be inserted into email messages or other forms of electronic communication unless the message is encrypted.
7. Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
8. All temporary passwords must be changed at first logon.
9. If an account or password is suspected to have been compromised, report the incident to IT Services and immediately change all of the associated passwords.
10. Automated password guessing may be performed on a periodic or random basis by IT Services Management or its delegates. If a password is guessed during one of these scans, the user will be required to change it.

14.4.2. Application Development Standards

1. Application developers must ensure their programs contain the following security precautions. Applications:
    1. should support authentication of individual users, not groups.
    2. should not store passwords in clear text or in any easily reversible form.
    3. should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
    4. should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

14.4.3. Use of Passwords and Passphrases for Remote Access Users

Access to the University Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

14.5 Enforcement

Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

15.0 Guidelines for International students

Foreign students are defined as holders of passports of countries other than India. For such students, the rules, policies and procedures as described in this document will be applicable. However, additionally the following would also apply:

a. The student ids will be given a broader degree of access to the Internet. Specifically, this access would include access to all websites (except pornographic in nature) without any debarring of any kind of sites, and access to Voice/video over IP facilities such as Skype.
b. Access and support on mobile devices such as smartphones, tablets etc.

c. Should the student have any application or device that is not covered by (a) and (b) above, the student should approach the IT Operations in-charge at their respective campus and provide specifics about the application / device. All reasonable efforts would be made to enable access for the same within the framework of the rules.

Additionally the students are advised to ensure the following on their device:

1. Ensure your operating system (OS) (Windows or otherwise) is legal

If you are using an "illegal" (unpaid, borrowed, or otherwise unlicensed) copy of Windows or other OS, your network login will not be successful and you will not be able to use UPESNET until that issue is resolved. If you have a PC with Microsoft Windows, you should bring legal Windows software CDs with you to the University, or you may have trouble connecting to the network.

If you do not already have legal Windows CDs, please purchase Windows before you leave your home country (and bring your Windows CDs with you)

OR

be prepared to purchase an English-language version of Windows when you arrive.

2. Make sure you are running the current Windows service pack

Once you do have a "legal" version of Windows, you should turn on Automatic Updates and allow any updates that you're prompted to do.

3. Remove viruses and spyware

Please do what you can to remove viruses and spyware from your computer before you try to use UPESNET.

15.1 Using UPESNET

15.1.1 Use DHCP to obtain an IP address automatically

As a student at UPES, you should never have reason to set a static IP address. Once you have properly registered on the network, an IP address will be assigned to you. Giving yourself (or any friends you are helping) a specific IP address will disrupt your network access in the long run, even if it seems to work initially.

15.1.2 Using wireless

The University wireless network is accessible from most of the common areas across the campus, including hostels and other accommodation facilities. When you are on campus, the wireless SSID you should be using is UPESNET (802.11x). You cannot run an independent wireless access point on the UPES campus.