IT POLICY

UTKAL UNIVERSITY

COMPUTER CENTRE

Contents

IT Policy of Utkal University

Preamble

Utkal University's Computing Facilities are related to symbolic computations, communications and network access, but not limited to, e-mail and Internet access. Computer Centre (CC) provides these services to facilitate the research, education and administrative efforts of its members and staff. To this end the Computer Centre (CC) provides support in networking and information resources for its teaching as well as administrative community. The Computer Centre undertakes security and monitoring measures to preserve the integrity and performance of its networking and computing resources.

Use of any UTKAL UNIVERSITY technology resource can be made by authorised persons as long as this usage is in compliance with University IT policy and all local, state and central government laws governing telecommunication. Failure to comply may result in the closure of an account, with further discretionary action taken by the Vice-Chancellor of the University, if necessary.

In order to protect the integrity of the UTKAL UNIVERSITY communications network and its systems, any proof of unauthorised or illegal use of any UTKAL UNIVERSITY network device and/or computer and/or its accounts can warrant an investigation. Users may voluntarily cooperate with the Computer Centre staff in such investigations. If necessary, User's files, accounts and/or systems will be investigated only by a person, persons or a committee designated for each case separately by the Vice Chancellor of UTKAL UNIVERSITY.

Policy Abbriviations and definitions

The following items describe general abbriviations and definitions of UTKAL UNIVERSITY's IT Policy.

Purpose:

computing facilities are to be provided by UTKAL UNIVERSITY and its centres, departments and Centre of Excellence or Schools in support of the research, teaching, administration and public services according to the mission of the University.

Users:

users of UTKAL UNIVERSITY computing facilities are to be limited primarily to UTKAL UNIVERSITY's academic and other staff, students and visitors for purposes that conform to the requirements of the item above.

IT Resources:

IT resources includes any Software, Hardware, Networking and other assets owned or hired by the university, intended to be used for IT based applications and services.

Entities:

Entities means and includes all Academic and Administrative units of University, Academic Service Units and all such units within or outside University which use Information Technology (IT) resources of the University.

Abbreviations:

CC: Computer Centre, Utkal University

Prof. I/C: Professor In Charge, Computer Centre.

Asst. Prof. I/C: Assistant Professor In Charge, Computer Centre.

System Manager I/C: System Manager In Charge, Computer Centre.

Responsible Uses of IT Resources

Policy Statement

UTKAL UNIVERSTY requires_employees(permanent /contractual) who use its information technology resources to do so in a responsible manner, abiding by all applicable laws, policies, and regulations.

Policy Scope

All users of UTKAL UNIVERSITY including guest users.

Policy Information

UTKAL UNIVERSITY employees are provided computing, networking, and information resources for use as business tools to support their efforts to meet their employment-related objectives. In keeping the view of freedom with responsibility, employees assume responsibility for their appropriate usage and are responsible for exercising good judgment regarding the reasonableness of personal use. Individuals are expected to be careful, honest, responsible, and civil in the use of computers and networks. Employees must respect the rights of others, respect the integrity of the systems and related resources, and use these resources in strict compliance with the local, state, central government laws, university policies, and contractual obligations. Using IT resources in the work environment in a manner that results in inappropriate conduct will be addressed as an employee performance issue, even if such conduct does not rise to the level of a university policy violation. Any use of university computers and networks by employees that is inappropriate to the workplace, or otherwise contributes to creating a harassing or uncomfortable workplace, or creates a legal risk, will subject the employee to counselling, formal disciplinary action and/or termination.

The university reserves the right to restrict the use of its IT resources and to remove or limit access to IT resources as required.

Misuse

Any usage which contravenes local, state and central government laws or violates norms of UTKAL UNIVERSITY usage will be treated as misuse. Two specific categories of misuse are listed below. All listed actions and others which effectively amount to the same are considered to be misuse of UTKAL UNIVERSITY's computing, communications and network facility.

Misuse involving or amounting to attack on any devices, systems and/or networks

1. Using the network to gain unauthorised access to any computer system.
2. Tapping phone or network transmissions (e.g. running network sniffers without authorisation).
3. Knowingly performing an act which will interfere with the normal operation of computers, terminals, peripherals or networks.

4. Knowingly running, installing and/or giving to another user a program intended to damage or place excessive load on a computer system,
network device or network. This includes, but is not limited to, programs known as computer viruses, Trojan horses and worms.
5. Attempting to circumvent data protection schemes or uncover security loopholes.
6. Masking the identity of an account or machine.
7. Releasing a virus, worm or other program that damages or otherwise harms a device, system or network
8. Using UTKAL UNIVERSITY's resources for unauthorised purposes (e.g. using personal computers connected to the campus network to set up web servers for commercial or illegal purposes).
9. Unauthorised access to data or files even if they are not securely protected (e.g. breaking into a system by taking advantage of security holes, or defacing someone else's web page)

Other categories of misuse

1. Using an account that the user is not authorised to use, or obtaining a password for a computer account without the consent of the account owner.
2. Providing any assistance to any person to facilitate unauthorised access to one or more files, accounts, computers, network devices or network segments.
3. Deliberate wasting of computer resources, but not limited to, like Internet bandwidth, CPU time, or excessively large (much more than 20-30 pages) print-outs. Please note that download of movies, music, on-line watching of movies or listening to music are disallowed. Download / upload using peer to peer protocol, visiting porno sites etc. is forbidden as is printing of text books, story books etc. Running of jobs not connected with UTKAL UNIVERSITY work/projects on computation severs is a similar deliberate misuse. Any other act not covered here will be discretion of the Professor I/C, Computer Centre.
4. Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing or deleting another user's files or software without explicit agreement of the owner.
5. Preventing others from accessing services.
6. Sending forged messages under someone else's name.
7. Employing a false identity for e-mail or other purposes.
8. Using email to harass others.
9. Charging the services availed of by a person to the account of another.

Wireless Security Policy

It is MANDATORY for departments deploying wireless network in UTKAL UNIVERSITY to implement secured access using one of the methods. Access to network/internet via wireless routers must be using one of the methods.

Wi-Fi Protected Access (WPA) OR Wired Equivalent Protection (WEP) AND Media Access Control (MAC) Filtering enabled access.

General guidelines to be followed are as below:

1. Provide the computer centre network group of your plan on wireless network deployment.
2. purchase only wireless access points and routers which comply to 802.1X standard.
3. Any user can reset the router to factory defaults and get access to router and network. Hence install the wireless router/access point in a secured place where physical access is not possible for general user.
4. Change the factory default administrator password of the wireless router/access point to a complex alphanumeric password.
5. Change the default Service Set Identifier (SSID) on all wireless routers/Access points to broadcast your department SSID s. This enables users to easily identify the access point to which they are connecting.
6. Deploy personal firewalls on all the remote access devices, such as laptops and enforce their continuous use. Ensure that user devices have up-to-date antivirus software security patches. Don't allow machines without protection on the network.
7. Enable DHCP server service on the wireless router using the IP range allotted to your department and disable the NATing feature on the wireless router. This will help in tracing the misbehaving laptop connected to the wireless router.
8. Upgrade the firmware of wireless router and access point as and when new security patches or new versions are released.
9. When disposing access points that will no longer be used, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.

Infractions

The following actions will be taken in case of infractions of the UTKAL UNIVERSITY policies:

1. All cases of infractions of this policy and misuse of UTKAL UNIVERSITY computing, communications and network resources will be logged and a written record will be kept with the Computer Centre. Such reports can be used to take further action if necessary.
2. Minor infractions of this policy or those that appear accidental in nature will be typically handled informally by email or in-person discussions. If an infraction has been judged to be accidental, a note to this effect must be made in the log with the Computer Centre.
3. More serious infractions will be handled via formal procedures.
4. In case of misuse involving or amounting to attack on any devices, systems and/or networks, if there is any need for immediate response, then offending accounts, computers, network devices or network segments will be isolated or shut down according to reasonable technical criteria. Such decisions must be taken by the chairman of the advisory Committee in consultation with the Professor I/C of the Computer Centre. Justification for these steps must be recorded after the fact in the log kept by the Computer Centre.

Server Account Policy

Accounts on CC servers are broadly classified as personal and official. The policy is defined for each category of users coming under the broad classification.
Nomenclature used for categorizing the accounts on servers is given below
a) Account given on Mailhost server for an individual, is called personal e-mail account
b) Account given for hosting an event is called official account.
c) Account given in the name of position, like Registrar, Chairman, Director etc. is called position account.
The policy is subject to modifications from time to time after necessary approval from Advisory committee of the Computer Centre.

A. Defined policy for Computer Centre (CC) servers

1. Members of UTKAL UNIVERSITY may request a personal account on a CC server based on academic or administrative needs. Requests by persons not in UTKAL UNIVERSITY for accounts on CC servers will be entertained only under the following circumstances:

> 1. If they are representatives or employees of vendors who are helping to set up a utility for which a purchase order has been issued.
>
> 2. Members of other academic Universities in India, if they are collaborating with permanent faculty of UTKAL UNIVERSITY.

2. Personal accounts on Mailhost and Webserver will be given only to the Permanent/Regular employee of UTKAL UNIVERSITY with a valid employee code issued by the UTKAL UNIVERSITY administration and which exists on the Payroll of the University, when the academic or administrative need is documented. The CC will create and abide by a written standard operating procedure for creation and closure of these accounts. Persons who are not Regular Employee of UTKAL UNIVERSITY cannot have personal accounts on Mailhost or the webserver.
3. Members of UTKAL UNIVERSITY may be given a personal account on a CC server other than the mailhost only if they have a valid personal account on the mailhost. Persons who are not Regular Employee of UTKAL UNIVERSITY may be given a personal account on other CC servers only if the request is countersigned by the Registrar of UTKAL UNIVERSITY. For non-members in category 1.1, the countersigning member of UTKAL UNIVERSITY will be the person in charge of CC operations. For non-members in category 1.2, the countersigning member of UTKAL UNIVERSITY must be a faculty collaborator with a valid personal mailhost account. All requests for accounts by persons in category 1.2 will be forwarded to the CC for a decision.
4. All personal accounts are meant for a single person. For every personal account on the mailhost, mail should be deliverable to [accountName]@utkaluniversity.ac.in as well as [accountName]@utkaluniversity.ac.in.

5. Official accounts may be created on the mailhost, the webserver and the FTP server for

1. Events organized by UTKAL UNIVERSITY.
2. Positions within UTKAL UNIVERSITY.

In both cases, a complete list of people who will handle the accounts must be given as part of the account opening process. Each such person must have a valid personal account on mailhost. The CC will create and abide by a written standard operating procedure for creation and closure of these accounts.

6. Each account will have an expiry date on creation. The expiry and closure of an account will be automatic.

1. The expiry dates for personal accounts given to all UTKAL UNIVERSITY employees will be 6 months after the date of superannuation or termination of contract as computed from the data presented in University Website. Closure of a personal account will be accompanied by removal of all data on the webserver. The sole exception for automatic closure of an account will be for faculty accounts on the mailhost and webserver. These will be carried out according to the policy mentioned in the section-B of this document.

2. During the 6-month period between the retirement of a member of UTKAL UNIVERSITY and the closing of his/her mailhost account, an automated message should be sent to the sender of every mail received for the account stating the date on which the account will be closed, and the new address for the recipient, if it is available.

3. For non-member accounts created for the category 1.1, the account will be deleted as part of the acceptance process for the purchase.

4. For non-member accounts created for the category 1.2, the account duration will be mentioned at the time of creation and must not exceed 6 months.

5. Accounts for events will expire 6 months after the end of the event. Organizers may request extension by a further period of 6 months. The data on the webserver associated with the account will not be removed unless requested by the organizers.

6. Accounts for positions within UTKAL UNIVERSITY will be locked on the earliest date of retirement or end of employment of the persons handling the account unless it is demonstrated and documented that password have been changed so that no non-employee can use the account.

7. The Professor I/C of the CC may authorize the immediate closure of an account if there is a security-based need for such an action. This action will be automatically reversed within two days unless the CC retrospectively authorizes such action.

8. Data associated with accounts will remain on long-term backups. Such data can be copied and released to old account holders with the approval of the Professor I/C, CC.

9. Personal accounts held by any person, and official accounts handled by him/her will be automatically locked on detection of a violation of UTKAL UNIVERSITY IT policy. Further disposition of these accounts will be decided on according to the procedure laid out in the UTKAL UNIVERSITY IT policy.

B. Policy for superannuated UTKAL UNIVERSITY faculty members

Superannuated faculty members can hold their mailhost and webserver accounts as long as the user is active and wishes to continue it. Account holder will be requested to confirm by mail, every year on continuing the account. On receipt of confirmation from account holder for the e-mail sent from CC system manager, acknowledgement will be sent confirming the account validity for one more year. The account will be closed if there is no response from the account holder for the e-mail sent from CC System Manger.

C. Exception to the above policy

Account on mailhost, webserver, and FTP server can be given to following non-UTKAL UNIVERSITY members to carry out their work.

1. Chancellor Nominee/ Raj Bhavan officers deputed to Utkal University

2. Government officers deputed to Utkal University

3. Officer on Special Duty (OSD) on deputation

4. Financial Advisor (FA) on deputation

5. Any other officials working in UTKAL UNIVERSITY Rural Campus.

To process the request, the requester has to submit application to The Registrar, UTKAL UNIVERSITY with his/her office room number and department details through Professor I/C, CC. The account will be provided only after authorization of The Registrar, Utkal University through proper channel. The closure of account will be as per policy mentioned above.

Data integrity and confidentiality policy for System Manager/Network Administrators

The nature of their work gives System Manager/Network administrators complete access to almost all data preserved in, or passing through, systems and networks. The following guidelines should be strictly adhered to within UTKAL UNIVERSITY:

1. System Manager/Network administrators must not examine or modify user data of any kind except as authorized by the Vice Chancellor of UTKAL UNIVERSITY, or on the specific request of the user.
2. System Manager/Network administrators must not allow anyone else, including other system Manager/network administrators, to examine or modify user data of any kind, except when the others are authorized by the Vice Chancellor of UTKAL UNIVERSITY, or on the specific request of the user.
3. System Manager/Network administrators will track user metadata statistically only for the purposes of efficient service delivery, except as authorized by the Vice Chancellor of UTKAL UNIVERSITY, or on the specific request of the user.
4. Direct requests for access to user data, metadata, or other information, by external agencies, including law enforcement agencies, must be promptly redirected by recipient system Manager/network administrators to the Registrar of UTKAL UNIVERSITY. Guidelines 1, 2, and 3, above, remain in force even in such cases.
5. System Manger/Network administrators must insist that all users abide by the UTKAL UNIVERSITY IT Policy (maintained on the Computer Center's website).
6. In addition to the above guidelines, all system/network administrators must abide by the UTKAL UNIVERSITY IT Policy.
7. request for access to specific server or network log data has to be routed through the Professor I/C, Computer Centre with proper explanation.

IT Management responsibilities

Policy Statement

Computer Center, Utkal University would ensure a consistent and integrated approach in the management of IT functions within its purview.

Policy Scope

All the departments of UTKAL UNIVERSITY including administrative bodies/ entities.

Policy Information

Computer Center of Utkal University, through its Advisory Committee, would ensure the following:

1. Track IT projects to ensure that they are completed within budget allocated and meet deadline
2. Coordinate IT human resources within Utkal University for effective utilisation to achieve business objectives of each department, Examination, Finance and Administration entities.
3. Coordinate with IT Advisors, consultants and Security auditors and work in close coordination with Advisory committee.
4. For any software development or implementation within UTKAL UNIVERSITY, user functionality requirements, design and architecture should be reviewed and sign off by System Manager, Computer Centre, Utkal University.
5. To define IT plans/roadmap for Utkal University and their successful achievement
6. To create data dictionary and create data structure for basic entities like Department, College, Faculty, Course, Subjects and Students/ Scholars.
7. To create central repositories for related data especially for Examination entity.
8. To ensure that succession plans exist for key IT personnel and IT Vendor.
9. Help departments to set up source libraries of the code with version control.
10. Encourage departments to set up core team for IT development and implementation
11. To be aware of the capabilities of existing IT systems in UTKAL UNIVERSITY and be able to recognise opportunities and risk.
12. Try to get common hardware register and common AMC.