Akaki Tsereteli State University

Information Technology Management Policy&Procedures

Date of creation:
Late update:
Next update:

Amendments

№	Date	Note

Drawn up : **By Information Technology Assurance Services**
Approved: **Under the protocol №65(17/18) 01.03.2018 of ATSU Academic Board**

Kutaisi
2018

Contents

Terms

University Society- University students, all Faculty and Academic Staff,employers, consultants, contract workers, additional employees and groups of people to meet various needs;

Information- awareness of subjects, facts, events, concepts and ideas, which makes sense in an appropriate context;

Hardware Assurance- electronic and mechanical parts of computational systems;

Software Assurance-The aggregate of programs, procedures, rules and relevant documents required for the processing of information;

Computer network and network equipment-data exchange system created by electronic-technical equipment(network adapter, routers, switchboard, etc.

Information Technology-presentation, processing, consolidation, storage and search of information related to Engineering and Technological Science. Information technologies encompass hardware and software assurance of information and communicative means.

Computer (calculating) resources- assurance of all the hardware and software under the ownership or supervision of ATSU, wired and wireless networks and networking facilities;

Information resources- Information created / processed / disseminated / transferred by the University. In general, letters, statements, orders, documents, etc.

Computer- work station, server, desk, portable computing equipment;

Server- specially allocated hardware or/and software assurance, which define functioning of other devices; Database, file, internet, consumer and other services.

Data- in electronic form: facts, concepts, numbers etc. that is processed via computers or other electronic devices.

Data owner-the head of the service, faculty, department; in exceptional cases the data owner can be another person as well.

Data processing- actions carried out on data; creation, receiving, recording, saving, accumulating, organizing, altering, reading, cutting, pasting, composing, deleting, cancelling;

Computer report- personal record concerning workstation, networks, electronic mails, educational programs, websites, services.

User- any person working on data and has computer or e-mail accounts;

User's right - the ability to access computer resources that infers the actions to be performed on the data: reading, writing, performing, changing, administering.

Authorized user - member of the university community or any person who has a computer or e-mail account and is entitled to process university data;

Administrator user- University community members appointed by Information Technology (IT) Assurance service who are eligible for the access to computer and information resources(System Administrator, Administrator, Database Administrator, Software Administrator, Active Directory Administrator);

Personal Data - Personal data related to identification of date of birth, address, history of education and organization of charity, financial activity, family status, etc.

Confidential personal data- racial or ethnic origin of the person, his religious belief, political views, psychological perspectives, his criminal record;

Overall information- retaining information in its form while processing, transferring, covering, saving; ensuring data perfection and accuracy;

Access to Information- assurance of information access in compliance with consumer rights;

Information security - protection from accidental or intentional damage of information resources and risk, which may damage the information owner or customer;

Data Protection- a set of measures to ensure, Information integrity, confidentiality and accessibility;

Case / risk (incident) - Information security violation, real or likely possible event that will lead to violation of privacy.

Internetworking screen (Firewall), a network security system- Hardware-software complexity between computer networks;

Computer virus and malware - programs that have the ability to create a copy of their own programs, in other programs, in optical memory, in the part of the discs that are designed to hamper the computing and network systems ,delete files, break file files, violate data integrity, etc.

Computer resources within the common use - computer resources that don't require user authorization;

Intebet Protocol- (Internet Protocol – IP)- protocol of transferring data through networks;

Internet address(IP address)-The numerical size assigned to a computer network.

Electronic email- email receiving and sending in the computer network;

(Dynamic Host Configuration Protocol – DHCP)- is th e protocol of the network which is used to support IP protocol and other devices;

Operating System-Computer software that manages the computer hardware resources and software.

Server operating system - an operating system that manages server computers.

Router- a network device / program that transmits data between devices in different networks.

Introduction

To fulfil the academic and scientific mission, it's expedient to make modern information technologies, computer systems and programs, ternal and external network data, internet access available for the university community members.

Information technology management policy and it procedures represent the unity of university or computer and information resources under its ownership, which will guarantee protection of users' rights, classification of electronic data and information security.

Use of computer resources and network

Policy Objective

In order to fulfill university academic and scientific mission, it is of great significance to allow university community members have an access to information technologies, computer systems, and programs, Internal and external network data.

Distribution area

The policy applies to the members of the university community, who use university computer, network and information resources. In addition to this, every person who has access to University computer resources.

General provisions

Applied information resources that are under the ownership of the University must be in compliance with the mission and its values.

The new operating systems, office programs, database systems, Internet and local networks that work in the local network that are necessary for daily activities are purchased and /or licensed to be installed on computers that are under the supervision and ownership of the University.

Computer network or resources are available for authorized users. They use computer resources pertaining to their accounts. (see "restricting users' access to their account or their right of access")

The university, which usually does not check or restrict the material transmitted to the computer network, yet retains rights to monitor individual sessions, account files, Systemic problems, viruses and other malware and decide wether the user breaches the rights of using information resources. University is also authorized to monitor non-university computers in relation to their computer resources.

The University reserves the right to restrict the access to the university's resources in case the rules are violated when using the computer resources. The Users computer on certain occasion and in case of violation will be disconnected from University computer networks.

Guidelines

User responsibilities

The member of University community can use university computer resources temporarily. The university employee is obliged to have temporary computer equipment in the working condition, not to take it without the permission of the university administration or hand it to another person. In case of detection of hardware disorder, the employer is liable to timely inform the administration which will apply to its part to Information Technology Assurance Service.

The user is liable to protect and avoid disclosing information to the third person, since it represents confidential information for university (see "Data classification") and it is preserved in university computer resources.

Any operating system and / or deleting/setting of software programs, configuration designed for university's computer resources (service stations, mobile computing and other types of electronic telecom equipment) is carried out via Information technology service, or in special occasions by the invited highly qualified specialist.

A member of the university community is obliged to use software that is under the ownership and supervision of the University only for legal purposes that do not contradict the law of Georgia and the statute of University.

The user may limit the access right to computer resources. Provide the resources are not restricted; other users aren't eligible to view, create the copy of it, change or delete other users' electronic files. If any of the users forgets to close work area (sessions), then other user shall close it . Non-administrator users are forbidden to conduct any information resources monitoring for any reasons.

The usage of computer resources is regulated in accordance with the copyright law [1] (see Copyright of Information technology resources)

Computer University resources can not be used for any person's defamation and insult.

Students mustn't use Training technologies, messaging and bogging programs carelessly in an unacceptable way.

Users do not need to change the software parameters on any compatible computer resource.

Computer accounts, passwords and other personal data are attributed to individual users and its it is inadmissible to share it with other users(except for special cases). The user is

[1] Articles 6,19 – https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=16198#

responsible for using his account (see "Create and cancel user account"). The account owner is responsible for every procedure carried our during the authorization session.

Users mustn't fulfill and/or change the software parameters to access to computer resources.

The users are banned from any actions to prevent the computer protection of a computer system. For instance, use programs and systems to have access to passwords.

It's against the law to use computer resources with evil intention. Such activities are as follows:

- Users should not intentionally distribute damaging programs: viruses, worms and others;
- No program should be installed without the permission of Information Technology Assurance service;
- They should not scan computer ports;
- When using the net they shouldn't download network flow or impede its implementation;
- Users shouldn't carry out processing tasks that would be harming to learning/ researching and modelling purposes;
- User should't use e-mail to send chain letters;
- It's forbidden to use computer resources for entertaining purpose(playing games, web browsing)
- Unauthorized monitoring of electronic communications should not be carried out;
- Computer systems mustn't be used for for the purpose of personal commercial and financial gain.

Data Protection

The university provides uninterrupted access to the centrally stored files, reserve copies of backup archives based on the needs of University (except for common folders created for data exchange)

The University shall not be responsible for the protection of personal computer or Non-centered and / or insecure folders and data. The user has to protect himself his privacy and all the personal data requires to be saved in terms of reserve copies of backup archives.

There is a necessity to set antivirus software for all computer systems approved by Information Technology Assurance service.

The university tries to ensure data protection, create reserve / backup copies in case data erases or is damaged by accident, but it isn't responsible for damages caused by electricity, fire, flood, non-authorized access.

Threat message

The risk of university computing resources usage can be determined via actions or events, that can be threatening to data safety, integrity, or availability of computer resources. The user should inform the IT Assurance Service about the threat.

Sanctions

In case of infringement of the rules of use of information technology, IT Assurance service will terminate the use of relevant software and restrict user's right temporarily or permanently, if necessary, it provides the university administration with the relevant information.

Create and cancel user account

Policy objective

The policy for creating and canceling user account stipulates Identification regulation of University community members in terms of university computer resources and emailing.

Distribution area

The policy applies to members to the University community.

General provisions

In order to use computer resources and emails, there are user's ordinary and exclusive rights to access accounts (see "Restrict users' access to their account or their right of access")

Information Technology Assurance Service appoints the owner of exclusive rights (administrator); every other member of the university community has consumer account.

Guidelines

Creating user's account

Faculty members/ staff:

According to the list of new staff provided by the Human Resources Management Service, Information Technology Assurance service crates a computer and an e-mail account for each employee. A learning program account is created for the academic staff and it will be presented to the head of the faculty.

Students: From the very beginning, e-mails and learning program accounts are created as soon as the student registers.

Deleting an account

Faculty employees/ staff: In accordance with the list of ex-employees issued by Human resources services, IT Assurance service deletes relevant accounts;

Students: changing the student's status does not have any influence on email accounts. As a result of University graduation, suspension and termination of student status, the student will accordingly have restricted rights to University computer resources.

Create and use passwords

Policy objectives

Its main objective is to establish laws relating to creating a secure password, its use and protection.

Distribution area

The policy applies to members of the University community who have user accounts.

General provisions

Passwords seem to be the most important components for Information and network security. Creation, usage or protection of all forms of account by the user must comply with the policy.

Guidelines

There are various kinds of computer accounts (see "Creating and deleting user account") Administrator user's account password must be changed after every 60 days. Ordinary user accounts (computer, e-mail, and consumer) require regular password changes after every 90days.

Password is the text size. Each user receives one time password from the administrator and is obliged to change it during the first use.

While creating the passwords, there are several criteria to take into account:

1. It must contain big and small alphabet letters (For example, a-z, A-Z);
2. A password contains characters, Numbers, arithmetic operation and / or other characters , for example 0-9, @#$%^&*()_+|~- =\`{}[]:";'<>?,./);
3. Passwords must be at least 8 characters in length.
4. It shouldn't be any word of any natural language(the person's name and surname, the names of the animals, towns and other names, Computer terminology, commands, names of institutions and others; Birth dates, addresses, telephone numbers and more; The following words: aaabbb, qwerty, zyxwvuts, password, 123321, secret1, 1secret ,etc.);
5. We can use abbreviations in order to create passwords that are easy to remember.

In order to ensure the security of one's password, the user must:

1. The same passwords mustn't be used both for University accounts and other kind of accounts (For example, Personal email account);
2. One must not share University account passwords with Administration representatives, secretaries, coworkers or colleagues (even while being off work on vacation), and family members. Each password is private information.

3. Password must not be written or saved online by electronic email.
4. Password mustn't be sent by means of emails or any other kinds of communicative means;
5. it mustn't be mentioned;
6. Password mustn't be disclosed via password reminder;
7. "Remember" Parameter mustn't be applied;

Information Technology Assurance service employer may demand user password if necessary.

If employer suspects password disclosure he must inform Information Technology Assurance Service.

Restrict users' access to their account or their right of access

Policy Objectives

The policy determines unauthorized or/and computer resources protection rules.

Distribution area

The policy applies to members of University Community owning University Computer resources and email accounts.

General Provisions

User right represents the unity of rights to access computer resources, which involves activities to be carried out upon data: reading, writing down, completing, changing, administering.

Guidelines

Giving the access right to Information Technology: the user has an exclusive right to access to special resources, that is of great significance to perform other professional/academic duties. The rights are defined (changed or/and cancelled) by the head of the department. The user is not liable to use other computer resources without authorization.

Change of access rights: If the user changes the position and / or duties at the university, users' access right must be redefined. The user must use computer resources, only those objects, accounts, access codes, privileges, or information he is responsible from his positional perspective.

Account access sharing: a user must not share his passwords with others and he is responsible for all the account operations, for any action carried out by means of the computer, which is under the ownership of the University.

University Electronic email

Policy Objective

Policy objectives determine the rules how to maintain electronic mail management.

Distribution area

The policy applies to the members of the University community who own university email accounts.

General provisions

Electronic email is one of the most important internal and external communicative means for the members of the university community. The electronic email which operates under the domain @atsu.edu.ge, is the main property for ATSU and it might be used for work

purposes. Not reading the content of the letter, not receiving or deleting it doesn't exempt the account owner from any liability.

In accordance with the Law of Georgia on personal data protection, correspondence Individual replies by employees or students represent their private information and it is not subject to email content monitoring except in cases specified in the legislation.

If the account owner has any questions relating to how e-mail system works, he must address to his immediate supervisor or Information Technology Assurance Service.

Guidelines

Use of Electronic Account

Email application types include, but are not limited to:

- Communication between the University members and / or university business partners by means of personal responsibility; Introducing Information and as well as its sharing;
- Participation in educational, research and / or professional development activities.
- copyright infringement, intimidation, abuse and defamation, fraud, plagiarism, fraud, creation of illegal pyramidal schemes or dissemination of computer malicious programs and others;
-
- Reviewing e-mail accounts and files, creation or deleting accounts, without other people's permission
- Unlocking duplicate messages sent from unsolicited emails to emails, which are open-source sources of viruses and malware programs;
- sharing email account passwords or attempting to comprehend the password of another person or other person's email account;
- Using electronic emails for other purposes such as: Commercial activities, political campaigns, distribution of chain letters and etc.

Create Electronic Email account

The following types of electronic email accounts (see policy" Create and cancel user account "):

- Individual accounts of University staff and students. The report is formed by a combination of the name and surname, if the mentioned combination is busy; the sequential number (according to the sequence of registration) is added;
- Single structural unit(Faculty, department, etc.), Research, scientific, cultural and social projects and other special postal accounts are formed in agreement with relevant services and based on their application;

Suspension /cancellation of Electronic email accounts

The e-mail account is suspended in the following cases:

- Computer resources and network usage Policy violation by university community;
- Employees' dismissal from employment;
- Students' status termination and student mobility;
- Liquidation / reorganization of individual structural units.
- Misuse of University e-mail;
- Dissemination of information prohibited by this policy and the Georgian legislation;
- Access to the account by a third party.

In case of email account termination Information Technology Assurance Service is obliged to inform the user as well as the supervisor about it.

Restriction will be removed after the elimination of its causes and will be notified as the account owner and his direct supervisor.

Monitoring

With the permission of the university administration, Information Technology Assurance Service may monitor any official communication, including e-mail, if there is reasonable doubt of misuse or breach of IT technologies management policy.

The service can monitor the user's email account in the following cases:

a) For the continuity of university activities (for instance, in need of information while the user is unavailable)
b) For the diagnosis and treatment of technical problems related to the system;
c) Investigate possible improper use of email and if there is reasonable doubt about the misuse and it is approved by the investigation;

Data Classification

Policy Objectives

The objective of the data classification stipulates sorting the data on the level of its confidentiality, flexibility and criticality in compliance with data owners' demands. The rules on data protection are determined by means of data classification.

This policy applies to only electronic data and it concerns data owners, the members of the universiyu community, who are liable to use data and information resources.

General provisions

In accordance with the information security, data classification is carried out in terms of confidentiality and the level of influence on university activities. Any information should be categorized according to the following three levels of confidentiality:

Limited data: The data are classified as restrictive,whearas unauthorized disclosure, changing or destroying can lead to high risks for university activities. Restricted data is protected by state legislation and confidential agreements (for example a student academic year, extranet, financial information). The highest level of safety must be maintained especially for limited information.

Personal Data:

The data is classified as private, personal (medical records), students' academic records, students bank and financial information, whereas nonsanctioned disclosure, changes or destroying it can be threatening for university activities. Normally, all university data, which are not classically as limited or public data, must be attributed to personal data.

Public data:Data is classified, as public, when nonsanctioned disclosure, change or destruction can either cause or don't even small risk of threat.For example the kinds of public data are as follows: references, notices, schedule, newsletters, newspapers, magazines, web sites, scientific works, etc.

It's necessary to ensure low level of security when it comes to public data. High quality security is necessary to avoid non-sanctioned modification or destruction. Public data is available to the member of the university community and other users as well.

Data Protection

Policy objectives

The policy aims at saving, processing and information resources and protection of transmission confidentiality, integrity and availability.

Distribution area

The policy applies to the mebers of the university, who have an access to information resources and systems.

General provisions

All the data and information system should be secured in accordance with the confidentiality, values and necessities.

Guidelines

Having access to information resources is defined by employee rights (see “Restrict users' access to their account or their right of access”)

The user shall obey the restrictions approved not only by the university but also by other users as well as the restrictions imposed by the third party, which do not contradict the Information technology management policy.

Copyright

Policy objectives

The purpose of the copyright policy is: software, databases and other electronic formats (literary, musical or artistic works, photographs, Libraries, video conferencing, etc.), which is protected by copyrights, protection of the creators' intellectual property and aims to reduce the harms associated with the breach of copyright law.

Distribution area

The policy applies to the members of the University community, who have access to university computer networks and resources.

General Provisions

There are purchased and/or licensed operating systems, office software, consumer applications, database management systems, required networking programs for the computers owned by the University that are necessary for everyday activities.

The University shares the requirements of the Georgian Law on copyright and neighboring rights. [2] Software and database in the university computer network either belongs to or is licenced by the university or the third party as well as approved by copyrights, Licensing and contracts rules and other laws.

The user is obliged to respect and protect the software and distribution licensees that contain the following prohibitions:

1. Create a copy of programs to use in the university network and distribute it outside the university;
2. Unauthorized downloads of copyrighted material protected in the university computer network and / or by means of other source of resources ;
3. data and/or software selling
4. Use of software for non-intellectual purposes and / or financial profits;
5. Public disclosure of programs (e.g. software code) or data without the permission of their authors / owners.

When it comes to the University networks, every user is obliged to protect copyrights of the works which are available under the terms of the Agreement on the Web site. If the user does not comply with specific copyright law, this does not mean that the copyright does not apply to this work.

[2] Articles 6,19 – https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=16198#

Sanctions

Policy objectives

The sanctions policy describes the University Information Technology management policy or/and sanctions imposed upon the members of the University community in case of violation of any applicable statute.

Distribution area

The policy applies to the members of the university community who have an access to University computer networks and /or resources.

General provisions

In case of infringement of IT management policy information technology assurance service terminates information service immediately, which may include the limitation of the user rights (see "User's Rights and Restriction"), termination or abolishment, and if necessary, providing information about the violation of the University administration.

Protection from malware and viruses

policy objectives

Protection from malware and viruses policy aims to remove malware (Trojan horses and worms) and viruses.

Distrinution area

The policy applies to the members of the universit community having access to networks and /or resources.

General Provisions

The viruses and malware , whic are designed to destroy electronic information, stealing and modifying information and for other harmful activities threatens the university's security of safety.

Guidelines

On the recommendation of the Information Technology Assurance service special software for the protection from malware and viruses and appropriate parameters shall be installed on any workstation, computer, file or web server, e-mail system which is connected to the computer networks in order to detect malware and remove them.

The software for the protection from malware and viruses mustn't be off. Its parameters should not be changed to reduce the protection effectiveness. The frequency of automatic updates of these programs should not be altered; particularly it must not be reduced.

The Information Technology assurance service should be notified about automatically detected and removed viruses as information security threat.

Use of mobile devices

policy objectives

The policy of mobile devices defines the use of university resources for smart phones, tablet computers and other mobile devices.

Distribution area

The policy applies to the members of the university community who have access to computer networks via electronic mails and electronic devices;

General Provisions

The mobile device is a small size portable computer that has many functions of the desktop computers.

Guidelines

It is necessary to consider the following while processing computer resources data via mobile devices:

- Use password-protect mobile devices to protect University data.
- Formation and use of Password must be followed in accordance with the Policy "Create and use passwords";
- The relevant operators as well as University Information Technology Assurance service should be informed about the lost, stolen or displaced mobile devices;
- User is responsible for the use of mobile devices, even if it is the person who has given it to the third party;
- Wireless communication system of mobile devices should be properly configured or transmitted;
- Reserve the data backup regularly to prevent delay caused by the loss or damage of the mobile devicere or chargeable battery. (see "Create a backup copy and data restoration" policy);
- The user is informed that when the mobile device and computer data are exchanged, the limited computer data on the personal computer is protected;
- Change the e-mail password if a mobile device used to access the University email has been lost.

Use of Portable Devices

Policy objectives

The policy aims at avoiding risk of loss /damage of university confidential information and spread of viruses and malware for the protection of computer networks.

Distribution area

The policy applies to the members of the university community, who use information resources to save and transfer their information via USB devices, optical discs, and any other physical media tools.

General Provisions

The portable devices, which can be connected to computer resorces, shall be used to save information. These kinds of devices are as follows: digital camera, external discs, etc

guidelines

The portable media devices should be checked via antivirus software recommended and approved by Information Technology Assurance Service. The device containing confidential data should also be physically protected.

At the end, user is obligated to disconnect the device at the most appropriate level protecting disconnection rules.

Create a backup copy and data restoration

Policy Objective

The goal of creating a backup copy and data restoration policy is to establish the reserve copy of the computer and information resources.

Distribution area

The policy applies to Data on the university computer and information resources.

General Provisions

It is important to create/restore backup copies and recover data files of the information resources the university owns.

Guidelines:

Reserve copies are created periodically and are kept safe. The purpose of storage:

- data restoration in case of software-hardware damage and force majeure;
- rectifying the accidental errors caused by users or damage caused by malware
- regular creation of reserve copies in compliance with the schedule provided by the IT Support Service.

Reserve copies can be complete and accumulative, which is created periodically. The standard procedures for creating backup copies are as follows:

- cumulative backups are created daily, are available for one week, and then destroyed.
- full backup copies are created once a month and are kept for 1 year;
- all the backup media devices have to be discarded as a result of one-time use, and the multi-purpose reserve media tools must be cleaned up;
- periodical inspection of backup copies is completed to maintain the integrity of data and to restore them in case of necessity;
- the schedule for saving backup copies is stored in the electronic document.

Electronic data management

Policy objectives

The policy determines to provide adequate management for computers and digital equipments the university owns: movement, repairing, writing off or restoring.

Distribution area

The policy applies to all the computers and digital equipments that are under ownership of the University.

General Provisions

Information Technology Management policy aims at protecting confidential information, ensuring fulfillment of software license agreements, that is why it's very important to manage electronic data on the movement of computer resources.

Guidelines

All computers and digital storage devices owned by the university should be treated accordingly, unless their ownership changes (such as, but not limited to selling, giving away, writing off) when processing computers and digital storage devices, all university related data as well as licensed software should be removed or get the device physically destroyed.

- All the computers and digital storage device the ownership of which is going to be changed should be sent to Information Technology Assurance service
- All employees of the university are responsible for the destruction of single digital storage devices. Single storage devices should be destroyed physically;
- If a hard disc is damaged or inactivated, it can not be used;It's necessary to dismentle and phisically destroy it.
- All PCs and storage devices that are to be written off are stored in a safe place;
- If the third party uses the university computer equipment, they should follow the university's electronic data management policy.

Internet Address Distribution

Policy Objectives

Internet address distribution policy aims at developing the distribution of the Internet addresses for computer resources.

Distribution area

The policy applies to all the devices connected to university computer network.

General Provision

The data transmission in the university computer network is organized by an Internet regulations, so all devices connected to it (must be given) are relevant (IP V4) address.

Guidelines

The distribution of computer (Internet) addresses (IP) is carried out by ITAssurance service. The devices with otherwise granted IP addresses must be removed from the network.

- Information Technology Assurance Service has the right to access the IP address with any device connected to the network; Issue of static IP addresses will be discussed in advance by IT Assurance Service;
- The devices connected to the network must be granted dynamic and Static IP addresses. Dynamically IP addresses are assigned through a specialized network device or server involved in the university network (using the DHCP protocol).
- Information Technology Assurance Service controls the documentation concerning IP addresses.

Computer network monitoring

policy objectives

The purpose of the computer network monitoring policy is to define the rules for analyzing, describing, and recording relevant data that is transmitted between computers across the university computer network.

Distribution area

The policy applies to all members of the university community and devices that have access to the computer network.

General Provisions

The university retains the rights to inspect and review all of its computational systems and networks,including individual sessions and report files. The observation aims at detecting problematic issues concerning the network, viruses and malware to determine whether a user violates the Information Technology Management Policy or State Legislation

Guidelines

- All computer and communication tools connectted to the university network are subject to this policy, whether or not it is owned by the University;
- Monitoring of university network, internet communication or university computer resources can only be carried out by information technology assurance services.
- The user should respect the rights of other users in relation to his / her data and should not monitor the network monitoring.
- The authorized staff must not disclose the information received during the network monitoring process without the permission of the university administration.
- Monitoring records conducted by the Information Technology assurance Service is kept for analysis purposes.

Network Routing Protection

Policy objective

The policy describes the required minimum security configuration of the university computer network for all routes.

Distribution area

This policy applies to all the routes connected to university network.

Generatl Provisions

Information Technology Assurance Service is responsible for installing the parameters of all the routes, management, and monitoring and audit reporting.In addition, the service can discard routes that aren't installed by them.

Guidelines

There must be the following standards of safety for each route to be protected:

- Access password must be stored in encrypted form;
- Standardized SNMP protocol should be used for management and monitoring;
- An encrypted (ssh) channel should be used for remote configuration of the route;
- Route software update and any other scheduled service work that will cause the computer network to be blocked and that is why it must be carried out during non-working hours.

Server Protection

Policy objectives

The purpose of server protection policy is to set up configuration standards for the servers owned by university.

Distribution area

The policy applies to all the servers owned by university.

General Provisions

Operation of all server owned by the university is carried out by Information Technology Assurance Service. If necassary the server can only be added/discarded with the permission of the very service.

Guidelines

- Servers should be placed on the protected areas and must be accessible to authorized personnel because there is no alternative to physical security.
- There must be some active services on the servers that are necessary for its purpose.
- Security updates of the server operating system should occur regularly.
- It's important to maintain regular checking of all servers by an antivirus program and regular updating of its database;
- Current accounts should be checked periodically and all inactive accounts should be canceled, reports must be created and maintained by a standardized system (Kerberos, NTLM, LDAP, Active Directory, etc.).
- Special attention should be paid to prioritized reports that have unlimited rights to use the resources (root; Administrator). The privileged account passwords should be given only to the main administrators.
- All account password formatting should comply with the "Password creation and use" policy.

Protective screen usage policy

Policy objective

The policy is designed to explain the rules for the management and use of computer screen protectors and its configuration.

Distribution area

The policy applies to all the protective screens owned by the university.

General Provisions

All the connections based on the university computer network must go through a network protective screen.The exceptions must be defined and verified by Information TechnologyAssurance service.

Guidelines

- Protective screens need to be periodically checked, which should include configuration parameters, enable / disable service, permitedt connection and security measures.
- All network screens must be physically located in data centers and it should be available for those people, who are responsible to access to the Network Protective Screen. These reliable spaces should also have proper physical security facilities.
- All suspicious activities that may be unauthorized or attempted to violate security rules must be recorded in the journal.
- Information Technology Assurance Service is responsible for computer network related operations such as: installing, canceling, managing, monitoring and auditing.

Wireless Connection

Policy objectives

Wireless connection policy is designed to explain the rules for safeguarding the most effective use of wireless network, safety and data integrity.

Destribution area

The policy applies to any equipment connected to internal network via wireless communication means(for instance, laptops, tablets, smartphones,game consoles,wireless projectors,etc.)

General Provisions

The management, monitoring and exploitation of wireless networks at university is carried out by Information Technology Assurance service.

Guidelines

- Access to wireless networks may be free or limited;
- Whether wireless networks are limited or free, access requires WPA2 / PSK technology and AES encryption using the appropriate password, so that transmitted data across this network is thoroughly protected from unauthorized access;
- Passwords that connect to Wireless Network are provided by the Information Technology Assurance Support Service.
- Password for free access may be given to anyone interested, put up on the news board or place it on any visible place
- password for limited wireless network is given to the members of the university community who need access to the network based on their work-related activities and they don't have right to disclose the password without the consent of the Information Technology assurance service.

Access to wired and wireless networks

Policy objective

The policy objective is to ensure the safety and security of wired or wireless networks and to provide unauthorized access to them.

Distribution area

The policy applies to all wired and wireless networks in University area.

General Provision

Wired and wireless networks are available for Information Technology assurance service and persons authorized by this service.

Guidelines

- If this is not possible, then network equipment should be placed in a locked room;
- Information Technology Assurance service staff or the people authorized by the service have physical access to the network equipment placed in the closet
- The network equipment must have adequate environmental (temperature, humidity, etc.) conditions and uninterruptible power supply.

Privacy protection

Policy objective

The policy provides guidelines for responsible management of the access to University information resources and data.

Distribution area

Members of the University community, who have access to university computer networks and resources;

General provision

The university computer network belongs to the university and uses it for academic, research and administrative activities.All the information in the network is(personal) private. Although the access rights to university computer network is strictly limited, the privacy is not guaranteed.

For the security of computer resources and its user accounts, the university uses all security measures. Despite this, the university finds it difficult to provide data safety absolute protection of users' privacy. Therefore the user should support "Secure Data Use",protect their accounts himself in accordance with "Creating and using a strong password" policy.

Guidelines

The user should know that the university network and computer resources are not absolutely private property. Although University doesn't monitor the use of individual information, normal functioning of the university network and information resources require creation of reserve backup copies of the necassary data and communications, caching data, keeping accurate attendance records, monitoring general schemes of consumption,etc.

The university may monitor the activities of individual users of the university network or cooperative resources, and the individual sessions and communication content of the event without prior notice when:

- User voluntarily makes available to all people the information that is placed by internet resources, web-pages or blogs;
- It is necessary to ensure the unity, security and functionality of the university resources;
- There is a doubt that the user has violated or violates the university Information Technology Use policy;
- It seems that the user's account is unusually active,which is against their rights.

Any of this kind of monitoring , Except as otherwise required by the user or by the law,or needed to react to the emergencies, should be allowed in advance by the head of the Information Technology Assurance Service. The university to its part, can disclose the results

of such general or individual monitoring,including the contents and records of individual communications according to the demands of the University or law enforcement agencies and impose the appropriate sanctions in compliance with the Universal Regulations.