Operation Principles of Information Technology Services at METU Campus Network

1. Purpose

This document is prepared in order to designate the operating principles of the information technology services for the server computers connected to the METU campus area network and provided by the units (academic and administrative corporate bodies functioning within METU).

2. Acronyms and Definitions

CC: The Computer Centre

DNS: Domain Name System

TCP/IP: Transmission Control Protocol / Internet Protocol.

IP address: Internet Protocol address. The IP Address formatted as 144.122.xxx.xxx, of each and every computer connected to the METU campus area network. Communication at METU campus area network is maintained by IP.

MAC address: Media Access Control address. The unique identification information set by the manufacturer on the network access card of any computer.

DHCP: Dynamic Host Configuration Protocol. This is the protocol that provides the IP and other information to be picked up from a server for the computers in order to access the network.

Port: A virtual gate way that is defined for the operating system and software of a computer to communicate within itself and with the operating systems and software on other computers via the network.

Patch: The software developed by the manufacturers to overcome the defects arising with the software or to be able to add new properties to the existing ones in the software.

Server system: The operating system and the software running on the server computers.

Security threats: The various methods (viruses, Trojan horses etc.) that spread wide due to security breaches, providing illegal access to data and thus threaten security of information and network access.

Services: The services (e.g. e-mail, web etc. services) aimed at the end users (clients).

Computer Coordinator: The person(s) responsible for the information technology infra structure of the units and who provide inter communication of the units with the CC regarding matters of the information technology infra structure.

Service Attendant: This is the person at the unit who is responsible for the operation of the server system.

Data traffic: The stream of data on the campus area network.

3. The Scope

This document depicts information regarding the installation, security safeguarding (security settings) and the operating principles of the systems that function as servers for the computers connected to METU campus area network. It is crucial that the installation and settings be performed in accordance with the ones stated in this document, so that the campus area network can be maintained properly and the security of the corporate / personal information in the computers connected to the network can be sustained. The units are responsible for following the principles stated in the METU Information Technology Resources Use Policy Document (http://computing-ethics.metu.edu.tr) for the services they provide.

4. The Policy

1. Prior to the decision of providing information technology services within their body, the facilities provided by the CC should be evaluated (http://www.bidb.odtu.edu.tr), and the services given by the CC should be preferred to be used primarily.

2. In addition to the central services provided by the CC, the units may provide further services in accordance with the general principles given on this document and in the framework of purpose specific principles residing at the specific document.

3. The units are expected to provide services in parallel with the directives scripted and announced by the CC.

4. The units have to inform the CC of their **Computer Coordinators** in writing and keep that information updated. They also have to provide the Computer Coordinator with information about the services they provide and the responsible person (**Service Attendant**).

5. The units are responsible for taking the necessary measures to provide the security of the operating system and the server software running on the servers.

6. For the services that they provide, the units are responsible for setting the standards of these services in accordance with the principles stated in the METU Information Technology Resources Use Policy Document (http://computing-ethics.metu.edu.tr), taking care to avoid conflicts, providing the documents of the rules to be followed and announcing the principles to be obeyed to their users.

7. The units are responsible for taking the necessary measures to keep their data traffic, which arise from the services that they provide, at a level so as not to cause an overload which would hinder the flow of data on the campus area network.

8. The servers at the units should, in no way, be meddled with without the consent and / or the knowledge of the Service Attendant and the physical safety of the servers should be ensured.

5. General Principles

For the information technology services they provide, the units are obliged to comply with the principals stated below.

1. **Reliable operating systems and software should be employed:** The operating system and the software running on the server computer has to be one which is technically and continuously maintained by the manufacturer or the provider, the security breaches of which are promptly announced and taken care of so that it is relatively immune to security threats such as, viruses and Trojans etc. It is common knowledge that open source code operating systems have more advantages, compared with the hidden source coded operating systems.

2. **The operating system and the software must be kept updated:** The operating system and the software used with the server computer must be kept updated and the announced patches should be applied on promptly (in order to keep track of the notices the related lists ought to be followed regularly).

3. **Access security should be ensured:** For cases where it becomes necessary to access the server computer remotely the IP addresses of access and / or the

users must be predefined and authorization of access must be given. Furthermore, access should be made via secure connections (for access terminal use ssh instead of telnet, for e-mail; imaps / pops instead of imap / pop, for file transfer; ftps instead of ftp etc.) right of access should be set to ensure access to certain authorized information and programs that elevate security (fire wall, TCP wrapper etc.) must be employed.

4. **Unused services must be shut down:** The services on the server computer not functioning any longer should be shut down due to reasons of probable breach of security.

5. **Server software with feedback should be preferred:** While choosing the software care should be practiced to make sure that it is software with communication lists where user problems faced can be conveyed.

6. **A backup policy should be set:** A policy should be set about the periodic back up of disk area where information belonging to the users and the service provided are kept and the users should be informed of the probable risks involved.

7. **Methods of user authorization must be set:** The rules related to the usage of the means (password access, IP based access, certificated access, smart card access etc.) which ensure access of the users to the services provided via the servers must be determined. For services where it is necessary to provide authorization with the central user codes, the authorization method standard which is decided upon by the CC (LDAPS etc.) should be followed.

8. **The server software should be operated in accordance with international standards suitable for the services to be given:** The services should function according to TCP/IP port numbers allocated by the IANA (Internet Assigned Numbers Authority) and at port numbers 1024 and below (http://www.iana.org/assignments/port-numbers).

9. **Installation and operation manuals should be read and documentation should be made:** All the manuals should be thoroughly read and installation and customization processes should be documented and archived at different locations before proceeding with the installation and customization processes. This system of precaution is vital for the services to be available to function as soon as possible in case of a probable failure.

10. **Logs must be kept and achieved on the servers:** The records of the services provided on the server computers must be logged and archived in accordance with the law and legislations.

6. Implementation and Sanctions

The Units are obliged to provide the services in accordance with the principles given on this document. In case of failure in complying with these principles, depending on the prevailing conditions, the CC has the right to apply the necessary sanctions, from notifying the Computer coordinator and / or the Service Attendant to temporary or permanent inhibition of access to the service, with, or without notice in cases of security related urgencies, in order for the campus network to function properly.

These rules are effective at the date of publishing. The authorities at METU keep the right to make the necessary amendments on this document when the need arises. Therefore, it is imperative that the users follow up the updated documents located at the "http://servis-ilkeleri.odtu.edu.tr" address.

ATTACHMENTS:

Atmt - 1: Service Specific Principles

1. E-Mail Services Operating Principles
2. Web Services Operating Principles
3. FTP Services Operating Principles
4. Data Base Services Operating Principles
5. DNS Services Operating Principles
6. DHCP Services Operating Principles
7. PC Room Operating Principles

Atmt - 2: Operating System Installation Principles for User Computers

Atmt - 3: Password Policy

Attm-1.1

E-mail Services Operating Principles

This document presents the principles for e- mail services provided by the units on their own server computers connected to the campus area network of METU and not on the central servers of METU, as an annex to the general principles and policies stated on the Operating Principles of Services Document.

The CC provides central e-mail services for personal and corporate users in METU. The units that would rather provide more disk space for their members or provide e-mail services with their own domain names instead of making use of the central e-mail services are responsible for primarily looking into and applying the set principles (see, Principles of Operating Services -> General Principles) related to the installation of the necessary hard and soft ware.

Besides the general principles, the specific principles, for those who choose to provide e-mail services as an alternative to the central e-mail services provided by the CC, are stated in the clauses below:

1. **Precautions must be taken against SPAM:** The e-mail server should be protected from becoming a source of SPAM. In order to stop the e-mail server to be used as a SPAM device the necessary layout must be set at the infra structure of the server and it should not be allowed to be used as an “open relay”. Furthermore, the SPAM filtration software, which is used to filter SPAM messages arriving at the mail server, should not filter messages which are not SPAM, therefore the configurations of the filtering software must be set to work according to this format / frame.

2. **Viruses that spread via e-mail must be stopped:** Virus filtration software must be incorporated and be kept updated in order to prevent viruses from spreading via e-mail messages. With such software, not only the outgoing but also the incoming e-mail messages contaminated by viruses ought to be filtered.

Attm-1.2

Web Services Operating Principles

This document presents the principles for web services provided by the units on their own server computers connected to the campus area network of METU and not on the central servers of METU, as an annex to the general principles and policies stated on the Operating Principles of Services Document.

The units that would rather provide web services on their own local network by their own means instead of making use of the central web services are responsible for primarily looking into and applying the set principles (see, Principles of Operating Services -> General Principles) related to the installation of the necessary hard and soft ware.

Besides the general principles, the specific principles, for those who choose to provide web services as an alternative to the central web services provided by the CC, are stated in the clauses below:

1. **A reliable programming language compiler and interpreter must be chosen:** Of the programming language compilers and interpreters available, the one with the relatively least security breaches must be preferred to run on the web server. It is imperative that, the latest and the most stable versions of the compiler and interpreter be used, probable security breaches be followed up and when a breach is detected, the necessary measures be taken and the corrections be made promptly.

2. **Reliable web server software must be chosen:** Of the web server software available, the one with the relatively least security breaches must be selected. It is imperative that, the latest and the most stable version of the web server software be used, probable security breaches be followed up and when a breach is detected, the necessary measures be taken and the corrections be made promptly.

Attm-1.3

FTP Services Operating Principles

This document presents the principles for FTP services provided by the units on their computers connected to the campus area network of METU, as an annex to the general principles and policies stated on the Operating Principles of Services Document.

The CC of METU provides two types of central FTP services for personal and corporate users in METU.

1. **Anonymous FTP services:** The anonymous FTP service is open to the entire Internet world and incorporates desktop applications that the users may need and the mirror images of some popular FTP sites.

2. **Licensed software FTP services (ftp.cc.metu.edu.tr):** The licensed software FTP service is only available to the staff residing in the campus and campus wide licensed software can be accessed via this service.

The units that would rather provide FTP services on their own local network by their own means, instead of making use of the central FTP services, are responsible for primarily looking into and applying the set principles (see, Principles of Operating Services -> General Principles) related to the installation of the necessary hard and soft ware.

Besides the general principles, the specific principles, for those who choose to provide FTP services as an alternative to the central FTP services provided by the CC, are stated in the clauses below:

1. **The appropriate transfer mode should be used:** In order to avoid probable security breaches the passive transfer mode instead of the active transfer mode should be utilized.

2. **The restriction of right of access:** The access privileges of the users accessing the FTP servers should be restricted so as to prevent them from accessing other locations than the directories including the files.

3. **FTP services that are not anonymous:** For FTP services that should not be anonymous and which include licensed software, it is essential to make the authorization of users by using the user code / password dual and to ensure that the distribution of software is done in the framework of the license agreements. It is recommended to make use of SFTP or FTPS instead of the standard FTP data transfer protocol.

Data Base Services Operating Principles

This document presents the principles of operating data base services provided by the units, and not on the central server computers of METU, on their server computers connected to the campus area network of METU, as an annex to the general principles and policies stated on the Operating Principles of Services Document.

The units that would rather provide data base services on their own local network by their own means are responsible for primarily looking into and applying the set principles (see, Principles of Operating Services -> General Principles) related to the installation of the necessary hard and soft ware.

Besides the general principles, the specific principles, for those who choose to provide data base services are stated in the clauses below:

1. **User accesses should be regulated:** The right to access to the data base should be granted to the users who need to access the data base by the Service attendant and the access of unauthorized users must be prevented.

2. **The users must be classified according to their level of authorization:** Each data base user must be given the lowest authorization enough to provide her / him to perform the actions needed. For each specific data base running on the same server system there should be unique user groups and administrators formed. For instance, a user needing 'read only' right should be given the right to read and not the right to enter or change data, users with utmost right for the X data base, if there is no need, should not be authorized for the Y data base with the same right.

3. **The default users of the data base management system must be inhibited:** The default users, with no passwords or low level passwords, designated by the manufacturer during the installation of the data base must be cancelled.

4. **The data base size quota must be designated:** A quota must be set in order to prevent over usage of disk space compared to the defined one and thus prevent probable service failure or lag.

5. **Access check must be performed for web based applications in reach of the data base**: Information like the IP address, user code and password authenticity of the web based applications for accessing the database must be supervised and a record of access must be logged.

6. **For the sake of data / password security, communication must be conducted via secure channels for cases where data access is on different individual servers:** The connections to the related servers must be done with SSH and the data base operations must be performed with "SSL – tunneling" for the security of data / password in cases of data base access on individual servers.

Attm-1.5

DNS Services Operating Principles

This document presents the principles of operating DNS services provided by the units, and not on the central server computers of METU, on their server computers connected to the campus area network of METU, as an annex to the general principles and policies stated on the Operating Principles of Services Document.

The CC already provides central DNS services so there is no need for the units to provide DNS services. However, the units that would still prefer to provide DNS services with their assets are responsible for primarily looking into and applying the set principles (see, Principles of Operating Services -> General Principles) related to the installation of the necessary hard and soft ware.

Besides the general principles, annexed are the specific principles, for those who choose to provide DNS services in addition to the central DNS services provided by the CC, and which the units have to follow, are stated in the clauses below:

1. **Zone Transfer property must be disabled:** If there is no secondary DNS server in use, the Zone Transfer property that enables the transfer of all the domain name and the IP correlation information, that the server harbors, to another client computer must be disabled.

2. **The Dynamic Name Server (DNS) property must be disabled:** Since it would cause security breaches, the DNS property, which enables the client computers to record themselves to the server automatically, must be disabled.

3. **Recursive domain name inquiries must be prevented:** The domain name inquiries received from client computers outside the unit must not be processed recursively, so this property should be blocked.

4. **Inquires from spared IP ranges should be disregarded:** The domain name inquiries that arrive from certain IP ranges (10.0.0.0/8, 192.168.0.0/16, and 172.16.0.0-172.31.255.255), which are spared for specific purposes, must be disregarded. There is a possibility that such inquiries may pose a threat for the general system security.

Attm-1.6

DHCP Services Operating Principles

This document presents the principles of operating DHCP services provided by the units, and not on the central server computers of METU, on their server computers connected to the campus area network of METU, as an annex to the general principles and policies stated on the Operating Principles of Services Document.

The IP distribution on the local area network is recommended to be static, which would bring system security and ease of follow up. However, the units that provide DHCP services with their assets are responsible for primarily looking into and applying the set principles (see, Principles of Operating Services -> General Principles) related to the installation of the necessary hard and soft ware.

In addition to the principles above **IP – MAC – user matching should be performed and the matching records should be kept in accordance with the laws and legislations** (IP – MAC – user matching should be defined on the DHCP server and it must be made sure that the computers accessing the network do this with their assigned IP numbers).

Attm-1.7

PC Room Operating Principles

This document presents the principles of operating public PC rooms provided by the units, and not by the CC, as an annex to the general principles and policies stated on the Operating Principles of Services Document.

The CC provides technical and administrative management of the PC rooms under its liability. The units that would prefer to run PC rooms with their own assets are responsible for primarily looking into and applying the set principles (see, Principles of Operating Services -> General Principles) related to the installation of the necessary hard and soft ware.

Besides the general principles, the specific principles to follow, for those who choose to set up their PC rooms, are stated in the clauses below:

1. **The rules for maintaining and utilizing the PC rooms must be set:** The units are responsible of preparing the rules for maintaining and utilizing the PC rooms they are running.

2. **The security of the operating system and the software used at the PC rooms must be maintained:** The operating systems used at the PC rooms must be configured so that there are no security breaches, the necessary measures against security threats like viruses etc. must be taken and if possible the necessary security updates must be performed in an automatic manner. The possible problems that may arise from automatic updates should be announced to the users and when the need arises updates should be turned off.

3. **A record of user traffic (in / out) to the PC room must be kept:** A record of the users who login / logout (the time range and the computer used) on the computers of the PC room must be kept (for a decent time period, to be looked up when necessary) by the unit running the PC room.

4. **The license agreements of the software installed at the PC rooms must not be violated:** It must be made certain that the software installed on the computers at the PC rooms be installed and used in the framework of the specific software agreement clauses.

Attm-2

Operating System Installation Principles for User Computers

1. Purpose

This document is prepared in order to designate the operating system installation principles for the user computers connected to the METU campus area network backbone.

2. The Scope

This document contains information and suggestions regarding the installation of the operating systems, security safeguarding (security settings) of the computers connected to METU campus area network backbone. It is crucial that the installation and settings be performed in accordance with the ones stated in this document, so that the campus area network can be maintained properly and the security of the corporate / personal information in the computers connected to the network can be sustained. The users are responsible for following the principles stated in the METU Information Technology Resources Use Policy Document (http://computing-ethics.metu.edu.tr).

3. The Policy

1. Users may install and use campus wide, personal / corporate licensed or free licensed (GNU/Linux, FreeBSD etc.) operating systems and software, as long as the principles stated below are abided.

2. The installation of the operating system ought to be done primarily from the updated operating system installation (CD/DVD or other etc.) sources that can be obtained from the CC Library, if provided. Alternative installations of the operating system may also be possible, provided that security is maintained.

3. It is recommended that the users get support from unit computer coordinators while installing the operating system and making the security settings.

4. General Principles

1. **The operating system must be kept updated:** It is necessary for the operating system and the software running on the operating system to be kept updated for protection against security threats. The necessary settings must be made

for the updates on the operating system to be performed automatically. The possible problems that may arise from automatic updates should be announced to the users and when the need arises updates should be turned off.

2. **Secure file system must be incorporated:** From among the file system options shown during the installation, the secure file system (for instance, instead of FAT32 or FAT, NTFS or EXT2) option, which provides facilities like right of access of users etc., must be preferred.

3. **User account passwords must be used:** Even if the operating system is in use of a single person, entry without a password must be prevented and it must be ensured that the users access the operating system with their own user accounts and passwords. Password access is crucial for the protection of the data in the computers connected to the network. The user account passwords must be simple, composed of alpha numeric and special characters (See. http://kullanicikodu.bidb.odtu.edu.tr → Kullanıcı Kodu Şifresi (Parola) Seçiminde Dikkat Edilmesi Gereken Noktalar).

4. **Antivirus software should be installed:** The most effective method for preventing viruses from disrupting the computers is to install and keep updated antivirus software. Keeping antivirus software updated is as important as installing one, since it can only detect viruses which have been defined. The information about the antivirus software that can be used under license within the campus may be accessed at METU antivirus web site (http://antivirus.metu.edu.tr/) address.

5. **The services that are not needed must be turned off:** Most of the security breaches arise from services working on the operating system under no supervision and the ports that are opened by these services. For this reason it is necessary to turn off services not being used.

6. **Backing up the information in the storage units:** Routine backups of the crucial information and the files of the users in the storage units will prevent the users from loss of information. The backing up media should not be coupled on to the storage unit of the operating system.

Password Policy

Below are the clauses about measures to bear regarding the usage of user account password dual when giving authority of access to the services (the access to the operating systems of the server and client computers, database access, web services access etc.) provided by the units.

1. **The security of the saved passwords must be maintained:** The necessary measures (like, not keeping the passwords as texts, building the necessary structures to keep them encrypted) to protect the passwords saved on the servers must be taken.

2. **Passwords must be checked against weakness:** Weak passwords should not be allowed when defining user account / password for the first time or for password changes and rules must be set for this purpose. For instance, the password must not have less than six characters, must contain at least three of the criteria; uppercase, lowercase letters, numbers and special characters and must not be a word out of a dictionary (See. http://kullanicikodu.bidb.odtu.edu.tr → Kullanıcı Kodu Şifresi (Parola) Seçiminde Dikkat Edilmesi Gereken Noktalar).

3. **Password update must be ensured:** Depending on how critical the service provided is, the password must be ensured to be changed at regular intervals.