Adopted by the Information Technology Center Management Committee
on December 11, 2013
Revised by the Committee on February 25, 2016

The University of Electro-Communications IT Systems Operations and Administration Procedural Manual

1. About This Procedural Manual

1.1 Purpose of the Procedural Manual

This manual identifies procedures pertaining to the appropriate operation and administration of information technology (IT) systems at the University of Electro-Communications (UEC) in conformance with Article 26 of UEC's Basic Operating Rules for IT Systems and the provisions in Article 41 of UEC's IT Systems Operations and Administration Rules.

1.2 Extent of This Procedural Manual's Applicability

This manual applies to everyone who operates, administers or uses IT systems belonging to UEC.

2. Organization That Operates and Administers UEC Information Networks and IT Systems

The Information Technology Center (ITC) is the administrative operation section that operates and administers information networks and IT systems at UEC as per the supervision of the chief information officer (CIO).

The heads of each domain are appointed to the domain supervisors who are responsible for domain supervision, and also appoint the persons below:

Domain Operations Managers
Domain operations managers are appointed from among personnel that belong to their specific domain, and are in charge of practical information network and IT systems operations and administration. They are allowed to appoint assistants from among the domain systems administrators.

Domain Systems Administrators
Domain systems administrators are appointed from among personnel that belong to their specific domain, and are responsible for operating information networks and IT systems belonging to their domains. Multiple domain systems administrators may be appointed.

Systems Administrators
Systems administrators are appointed from among the domain systems administrators, systems administrators assist the domain systems administrators with their work. Multiple systems administrators may be appointed.

For instance, within a department, the domain operations manager is responsible for operating the department's domain. The domain systems administrators serve as representatives of the systems administrators for each course in the department. The systems administrators are of the course themselves.

ITC primarily communicates with the domain operations managers. When assistants of the domain operations manager have been appointed, and the domain is being operated and administered by multiple personnel, however, a mailing list or other method must be prepared so that domain operations managers and their assistants can all read e-mails from ITC, in case of emergencies.

The following personnel are also involved in the operation and administration of information networks and IT systems:

IP Address Managers
The IP address Managers handle the administration of logical IP address blocks for the campus network. They are appointed from among personnel chosen by the system administrators who use those logical IP address blocks. ITC manages IP addresses if an IP address administrator cannot be selected.

Building Network Administrators
Building network administrators handle the administration of physical networks (LAN wiring and network devices) installed in each building.

These personnel, each department's domain operations managers, and domain systems administrators must cooperate with each other to operate and administer the information networks and IT systems.

3. Instructions for Accounts and Passwords

3.1 Passwords

Passwords are the most important means of protecting IT system users. As such, all passwords must fulfill the following conditions:

- Be a minimum of eight characters, and twelve or more characters if possible
- Include upper- and lowercase letters, numbers, and symbols
- Not be words found in dictionaries or proper nouns

Even if passwords are sufficiently complex, it is recommended that they are changed regularly. Furthermore, in the case of a partial data leak all passwords thought to have leaked are to be changed immediately, even if they were encrypted or hashed.

The temporary passwords provided to users must be changed within a certain period of time. Users must not be allowed to continue using their temporary passwords.

3.2 Using Accounts

Systems which have account features must create accounts for users. Multiple individuals must not share a single account, except in the case of an IT system that does not allow multiple accounts.

Account administration must be especially rigorous when a device (such as an inexpensive broadband router) has no multiple account features or has only one account with administrative privileges but is operated and administered by several people. Account information must not be divulged to personnel who are not involved in the system's administration and operations.

3.3 Active Use of Passwords

PCs have screen lock features that users can employ when temporarily stepping away from their workstations. Users must always lock the screen to maintain security when they step away, no matter how briefly. There is also a feature that makes entering a password compulsory for waking a PC from a sleep or standby state. These features must be used without fail.

4. Allocation, Administration and Use of IP Addresses

4.1 Types of IP Addresses

The following four types of IP addresses are allocated and used as needed on the campus network. ITC specifies the ranges of these address blocks.

- Global IPv4 address blocks
- Private IPv4 address blocks
- IPv6 address blocks

- Other special use address blocks

Allocation criteria are as shown below:

- Global IPv4 address blocks

These IPv4 address blocks are primarily allocated to servers that need to be open for communicating with off-campus networks directly. They must not be allocated to multifunction printers, printers, NAS appliances, network cameras, administration interfaces for IT devices or Internet of Things (IoT) devices. Sufficient oversight must also be exercised when allocating them to devices that hold personal information.

- Private IPv4 address blocks

Private IPv4 address blocks are divided into two types: those for which only on-campus communication is possible, and those that can only communicate within a physical segment of the network. These are allocated to clients that have no need to communicate directly with anyone outside the university, multifunction printers, printers, NAS appliances, network cameras, administration interfaces for IT devices, and IoT devices.

- IPv6 address blocks and other special-use address blocks

These IP address blocks are used for experiments and collaborating with institutions other than UEC as well as local communities. ITC allocates these as needed.

4.2 IP Address Allocation

The IP address administrator allocates IP addresses according to the following procedures:

1. Systems administrators that want to allocate IP addresses fill out an application form available at ITC and submit a request to the IP address administrator.
2. The IP address administrator carefully checks the applications. If there are no problems, the IP address administrator sends these applications to ITC. When private IP address blocks are requested, the administrator briefly check the application and allocates private IP addresses.
3. When applications for global IP address are requested, ITC carefully examines the application. If there are no problems, ITC notifies the IP address administrator that requested global IP addresses may be allocated. And then, ITC opens the firewalls to have external connections via those IP addresses.
4. Systems administrators configure and operate IT devices according to their applications, and record what they did in their ledgers.

5. ITC retains all applications.

4.3 Using IP Addresses

Systems administrators must promptly notify the IP address administrator when an IP address is no longer in use. In the case of global IP addresses, the IP address administrator must then notify ITC of this change. To prevent the illicit use of terminated global IP addresses, ITC must promptly change its firewall configurations after being informed by the IP address administrator.

IP addresses are allocated in accordance with requests. Systems administrators are not allowed to maintain inactive IP addresses. When IP addresses are allocated dynamically, an allocation system that matches the allocated IP addresses with their users should be used, and logs should be maintained.

5. Installing, Using and Disposing of IT Systems

5.1 Installing IT Systems

When planning to install IT systems, the following issues must be considered:

- Who will be the system's supervisors and administrators?
- Who will use the system?
- When will the system be used?
- Why is this system needed?
- What will the system be used for?
- Where will the system be used?

All IT systems must be selected after clearing these questions. The duration of the maker or vender's support for the following items must also be considered:

- Hardware
- All software required to configure and operate the IT system, including the operating system, antivirus software, and various other kinds of software

If the support provided is shorter in duration than the length of time the IT system will be in use, upgrades and updates must be factored into the plan.

Measures for IT systems that require high availability—such as multiplexing and enhancing support systems—must be implemented.

IT systems for which high confidentiality is required must be installed on locked racks in locked rooms whose keys are strictly controlled and positioned in such a way that no one but their administrators can physically reach them.

5.2 IT System Installation

IT system installation must be performed in the following sequence:

1. Gather the required information
2. Configure administrators' accounts and passwords
3. Update the operating system and firmware and initiate security measures
4. Install and update antivirus software
5. Install, update and customize various types of software
6. Configure the firewalls
7. Check operations
8. Document the work and enter it in the log
9. Give users access and monitor them

Changing the sequence of the work is allowed if it can be guaranteed that there will be no malware incursions. IT systems must be able to adequately withstand all known malware and attacks after the installation is completed. Data leaks must be prevented in the case of IT systems that contain personal information by using firewalls that restrict communication between the university and the outside campus.

Making backups of an IT system as needed is preferable. However, regular backups must be performed without fail on systems that must maintain high availability.

IT systems that enable log acquisition should always be configured to do so. Log retention periods will depend on the sizes of the fields to be retained, but being able to save them for a month is preferable.

ITC distributes Microsoft products and antivirus software products under campus-wide licenses. These licenses must be actively used to reduce costs when they conform to the conditions for use.

5.3 IT System Administration Tasks

IT system users must routinely undertake the following measures as IT system administration tasks:

5.3.1 Security Measures

Apply security update for operating system and application software
Configuring the system to enable automatic update is preferable. Systems administrators must instruct users on how to apply updates when such updates are released.

Updating antivirus software's virus definition files
The automatic update frequency should be set for once or more per day. Before they begin using IT systems, users must check their antivirus software to confirm that it is operating, and ensure that the latest virus definition file is installed.

Acquiring and checking security information for the operating systems and application software being used
Personnel must obtain updates for the operating systems and application software they use. Systems administrators must also have an understanding of how the operating systems and application software under their supervision are used. Systems administrators provide users with information of the most recent updates.

5.3.2 Checking Logs

Logs must be checked regularly to confirm that no illicit access or attacks are occurring. Instances of illicit access must be reported immediately and countermeasures must be devised. Logs must be checked when attacks are being blocked, and additional countermeasures must be devised and reviewed.
Read "10. Information Security Incident Responses" for more information about submitting reports.

5.3.3 Backups

Backup plans must be devised according to the level of importance of specific IT systems. Backups should be made regularly.

5.4 Tasks Related to IT System Termination and Disposal

The following tasks must be carried out when terminating an IT system. The termination work reports regarding the following tasks must also be submitted to ITC and IP address administrator when a system has global IP addresses:

- Transfer and backup information that will be needed thereafter
- Deletion of private/personal data
- Safety measure to ensure that the system is not used by mistake

The following tasks must be carried out when reviving IT systems that have been terminated. IP addresses must be allocated in the same way for a new IT system installation.

- Confirm the duration of support for all installed operating systems, application and antivirus software
- Update operating system, application and antivirus software. Apply other security measures
- Check that the personal data were deleted if the system will longer be used by different users. Whenever possible, format all hard drives and other storage media before reinstalling the operating system and applications.

The following tasks must be carried out when disposing of IT systems:

- Check the licenses of all software installed. Deactivate software license registrations whenever it is possible to do so.
- Delete all data stored on hard drives and other storage media before disposing of them. In the case of hard drives, use devices or programs designed to wipe hard drives, and then physically destroy the hard drives. CD-ROMs and other medias are to be destroyed with shredders or other devices.
- Follow the Financial and Accounting Office's instructions when disposing hardware used for the IT systems
- Record IT system disposal in ledgers

6. IT System Ledger Preparation

6.1 IT System Ledger Preparation Tasks

Ledgers pertaining to IT systems used in the specific course, lab or section unit must be prepared. The software being used on them must also be recorded on the ledgers. The following ledger items are required:

- IT systems

Hardware names; installation dates; equipment numbers; supervisor, administrator and user names; purposes of use; operating systems; IP addresses; places of use; and disposal dates

- Purchased software

Software names; numbers of licenses purchased; installation dates; numbers of usage licenses; names of the IT systems on which they are installed; and the places where media are stored

The IP address administrator must prepare an IP address management ledger for IT systems having global addresses that enable direct connections from off-campus. The IP address management ledger must also be shared with ITC, which oversees the administration of the ledgers. Follow ITC's instructions for sharing methods.

Hardware names; installation dates; equipment numbers; supervisor, administrator, and user names; usage purposes; operating systems; IP addresses; places of use; and a list of public ports

When global IP addresses are used for transmissions not recorded in the IP address management ledger, ITC and IP address manager may determine that the information networks are being used illicitly. And ITC will work alongside the domain operations managers and domain systems administrators to handle the issue.

Ledgers are to be updated whenever there are changes. The actual number of IT systems in use and in the ledger must match.

7. Handling Privately Owned PCs

Faculty and staff working for the university must not connect their personal PCs to on-campus networks or copy confidential UEC data to their personal PCs.

Students can connect their personal PCs to on-campus networks with the permission of domain systems administrators. However, domain systems administrators must confirm the following:

- That the PC has sufficiently strong security measures
- The status of update for the operating system and application software installed, and whether the virus definition file for antivirus software is up to date. Personal PCs that do not have the latest updates may not be connected.
- Whether the PC has peer-to-peer (P2P) file sharing software installed
  The use of anonymous P2P file sharing software is prohibited on campus. This type of software can automatically start up in the background, sharing files without users even realizing it. Domain systems administrators must check this aspect carefully.

It is preferable for students to connect their personal PCs to networks with restricted access; specifically, to private IP networks or networks with restricted access to ports. Barring a special reason such as research, these restrictions must apply to access ports for off-campus

communications when connecting personal PCs to Network Address Translation (NAT) routers to acquire off-campus connectivity.

8. Taking Out, Transporting and Saving Data

Information on the university affairs and other confidential data must not be sent or transported off-campus unless there is a particular need to do so. In cases where there is a special reason to bring the data, permission from the personnel responsible for domain supervision must be granted. In such a case, encryption that possesses sufficient strength must be applied. The following encryption methods must be used:

- Encryption folders that are a feature of operating systems
- Various kinds of software file and drive encryption

Additionally, using electronic signatures should be considered when maintaining data integrity is essential.

Confidential data must be encrypted and stored in a safe place whether it is saved on or off-campus.

Encryption keys must be saved and transported separately from these kinds of encrypted data.

9. Using Networks Other Than Campus Networks

Domain operations managers and ITC must be notified about any intention to use networks other than campus networks for research use or clerical work, except for the use of mobile telecommunications such as cellular networks and the wide area Wi-Fi.

Any route advertisement must not be allowed over campus networks, even for research purposes.

10. Information Security Incident Responses

When they detect information security incidents, the assistant IT systems security supervisor (hereinafter assistant security supervisor) and IT security advisor (hereinafter security advisor) take the measures needed to prevent further damage and to ascertain the causes.

- Blocking communications through relevant IT systems on and off-campus
- Cutting the connections of relevant IT systems to campus networks
- Requesting that the administrators of relevant IT systems investigate and respond

- Investigative interviews with the administrators of relevant IT systems
- First-hand investigations of the relevant IT systems
- Examination of the relevant IT systems' storage and other devices

The assistant security supervisor and security advisor will take the lead in responding to information security incidents with the domain operations managers and IP address administrator when information security incidents occur in university IT systems. The procedures for this are as described below:

10.1 Determining That an Information Security Incident Has Occurred

Confirm that an incident has occurred from log data on IT systems, including intrusion detection systems, public information, and notifications from off-campus.

10.2 Communication and Initial Responses to Information Security Incidents

Anyone who discovers an information security breach must tell that IT system's users to stop using it while at the same time notifying superiors, including the domain systems administrator and systems administrator. The domain systems administrator must then notify ITC, and the assistant security supervisor and security advisor need to confirm that an information security incident has occurred.

To prevent further damage, the domain systems administrator and systems administrator must then disconnect the IT system on which the breach occurred from campus networks, and do so without waiting for instructions from the assistant security supervisor or security advisor. In other cases, the assistant security supervisor or security advisor is to instruct that an IT system on which an information security incident has occurred be disconnected from campus networks.

10.3 Investigations and Responses

Domain systems administrators and systems administrators are to investigate the security breach according to the assistant security supervisor or security advisor's instructions.

The assistant security supervisor must compile a report following the responses to the information security incident and submit it to the IT systems security supervisor (hereinafter security supervisor, who is concurrently the CIO). The security supervisor may conduct interviews with the assistant security supervisor and security advisor, as needed before deciding how to proceed.

10.4 Steps to Prevent Information Security Incidents

The security supervisor must endeavor to prevent recurrences of security breaches, recommending improvements that address the causes of the incidents to all domain supervisors, and domain systems administrators.

11. IT Security Audits

The assistant security supervisor and security advisor must conduct regular IT security audits of the university's IT systems, gathering information about IT system vulnerabilities, and recommending improvements to the domain systems administrator and systems administrator when they discover vulnerable IT systems. Measures similar to those for information security incidents can be undertaken if improvements related to the relevant IT systems' vulnerabilities are not made.

12. Audits

The IT security auditor conducts regular internal audits of how domain operations managers and security supervisor run IT systems and maintain their information security.
Domain operations managers must instruct the domain systems administrators to cooperate with internal audits.
The outcomes of internal audits are reported to the CIO. The CIO must recommend improvements to IT system operations and the maintenance of their information security based on those results, maintaining a high level of information security on UEC's IT systems.

13. Information Security Training

The assistant CIO must create and implement plans for the regular training of faculty and staff in UEC's administrative and operations sections on the topics of information security and information ethics. The administrative and operations sections must prepare teaching materials on these topics that UEC personnel can present, and request that training on information security and information ethics be implemented regularly for individual sections.
The administrative and operations sections are also to request that each section conduct this training for their newly enrolled students. The administrative and operations sections can undertake measures—including halting the use of UEC information networks—to lock out users who do not attend the information security and information ethics training each section specifies.