CAMPUS OPERATIONS STANDARD PRACTICE

TITLE:	INSTRUCTION NUMBER:
Facilities Services Network Device-Installation, Modification, and Removal	**100-0083**

I. PURPOSE

The purpose of this COSP is to establish guidelines governing the use and connection of Facilities Services networking devices on the University's Communications Networks. This COSP applies to all Facilities Services networking devices, ranging from multi-user systems to single user personal computers utilized for physical plant operations and monitoring. Networking equipment includes, but is not limited to: controllers, instrumentation, meters, switches, hubs, routers, servers, wireless access points, blade server systems, virtual machines, and/or Virtual Private Network (VPN) devices, etc.

This COSP details the procedures and responsibilities to accomplish adherence to this policy as relates to the installation, modification, and maintenance of all devices used to operate or monitor the physical plant that connect to the University's Communication Networks. This COSP does not attempt to outline approval, review, or administrative procedures of the Information Technology and Computing Services (ITCS) Department.

II. GENERAL

To ensure compliance with all policies, additions and/or modifications to the Facilities Services' networked devices may not be done without the prior approval of the Facilities Services and/or ITCS Departments. This includes but is not limited to: the installation or modification of building automation systems, utility monitoring systems, water treatment systems, medical gas/vacuum systems, fire alarm systems, lighting control systems, equipment controllers such as smart valves, elevator surveillance systems, wireless devices of any type, and instrumentation. The security of these devices once installed is the responsibility of the requesting department, Facilities Services, and ITCS.

Violations of these policies will result in the termination of network service to the offending network device. In the case of a willful violation, violations will be handled in accordance with the applicable Computer Use Policy. Network abuse will be referred to the Associate Vice Chancellor for Campus Operations.

III. RESPONSIBILITIES

A. Facilities Services is responsible for notifying ITCS of any proposed installation, modification, or removal of any networked device before work begins.

B. Facilities Services departments are responsible for working through the Facilities Technology Support Manager for all installation, modification, removal, and maintenance of all networked equipment.

C. Facilities Services and Facilities Engineering and Architectural Services will ensure networking devices are pre-approved by ITCS Networking Services, prior to purchase in order to ensure that the device(s) will not have an adverse impact on University's Communication Networks. Pre-purchase engagement works to limit the potential issues or conflicts from the acquisition. ITCS is responsible for notifying Facilities Services of problem network device(s) and/or service(s) in a timely manner.

D. ITCS will assist departments of authorized equipment in resolving any problems with their devices. Any networked devices or services that are detected and verified to degrade the quality of service on University's Communication Networks, if not corrected will result in termination of network service of that device until the cause of the problem is corrected. Upon verification or certification of corrective action(s), the offending system will be re-admitted to the University's Communication Networks.

E. If Facilities Services finds that a new or upgraded system cannot meet security requirements, Facilities Services is required to take alternative precautions to reduce the risks to acceptable levels. For example, if a new system is unable to enforce University password requirements at user login, Facilities Services should establish a departmental password procedure, train Facilities Services staff on the procedure, and regularly remind Facilities Services staff of obligations under the procedure.

F. The Facilities Technology Support Manager will maintain a software "patch strategy" for Facilities Services networked devices that is aggressive but still achieves an appropriate balance between system stability, data security, and service availability.

G. Facilities Services Department Managers shall assess privilege account use and annually review privileged access rights to ensure that Facilities Services staff have only the access needed to carry out duties. Facilities Services Department Managers are responsible for promptly revising privileged access rights when such rights are no longer needed.

H. Facilities Services will grant privilege access for contractors and other staff on an as needed basis and promptly revoke the access when it is no longer needed. To reduce the window of exposure, Facilities Services will grant privilege access for specific times that coincide with a particular task schedule and revoke the access afterward.

I. Facilities Services Supervisors will work through the Facilities Technology Support Manager and ITCS to establish temporary remote access via a VPN when remote access is required.

J. Documenting access rights: To keep track of the assignment of privilege access rights, the Facilities Technology Support Manager will centrally document VLAN privilege access rights in the ITCS database Infoblox. Additionally, all shared passwords will be maintained in Keeppass a password database

K. The Facilities Technology Support Manager in collaboration with ITCS Network Analysis and the Facilities Services Supervisors, will review access privileges on an annual basis.

L. Facilities Services shall enforce University passphrase requirements at user login for password length, complexity, expiration, and reuse at the server and front end system level. If the system is not able to do so, the Facilities Services department will contact the Facilities Technology Support Manager for guidance. Facilities Services will establish a process for securely communicating new and temporary passphrases with users. Facilities Services will promptly change default product and vendor account passphrases to prevent unauthorized access.

1. ECU passphrase requirements at login:
   - Passphrases shall be at least eight characters in length.
   - Passphrases shall contain characters from at least three of the four character classes: numeral, upper case letter, lower case letter, and special characters (!, @, #, *, ?).
   - Passphrases shall be changed at a minimum of once every 90 days and shall not use any of the user account's previous six passwords

M. Alternative controls: If a system cannot meet University passphrase requirements, Facilities Services must implement alternative controls to provide an equivalent level of access control security. Unfortunately, it is not uncommon to find that a product lacks the necessary enforcement controls. For example, a specialized software application may limit passwords to six characters or less, which prevents users from selecting passwords that meet University requirements for minimum passphrase length. Examples of alternative controls include:

1. Using highly complex passwords (when password length is an issue).

2. Working with the software provider to provide a fix that allows strong passwords.
3. Switching to a different product altogether.
4. Limiting access to the product from specific end user devices.

N. The Facilities Services Supervisors will notify the Facilities Technology Support Manager of any updates for networked devices where a shared password is utilized and ensure that the shared password database is updated.

O. Legacy password systems tend to focus primarily on password complexity and less so on password length. Because password strength is based primarily on complexity and length, legacy systems often result in short, complex passwords that are difficult to crack and difficult to remember. Fortunately, within this framework, user can also use a different type of password, known as the passphrase, which is easier to remember and just as secure. A passphrase is a longer version of the password and relies more on length than complexity. Departments can create a passphrase from a word phrase or sentence, yielding a passphrase of ten characters or more in length. By using mixed-case characters and adding a numeral or special character, a passphrase can be easy to remember, yet very difficult to crack.

P. Default and vendor account passphrases: Default product and vendor accounts and default passphrases are well known and frequently sought out as a simple means to gain unauthorized access to a system and an institution's network. Therefore, it is important that departments disable default accounts and change default passphrases at the earliest possible moment during implementation or maintenance.

IV. PROCEDURES

A. Facilities Services staff shall be provided with access to only those data, applications, network resources, and physical locations necessary to perform job duties and responsibilities. Where practical, job duties and responsibilities shall be separated to reduce the risk and impact of security incidents that may cause material or operational disruption to the University.

B. User access rights shall be authorized by the appropriate management authority prior to granting access to critical University systems. Access rights shall be documented in the Infoblox database maintained by ITCS. Authorized users shall be assigned unique user accounts, wherever possible, so that user activities may be associated with the specific user.

C. Wherever shared user accounts are necessary to access critical University systems, a risk acceptance shall be documented, reviewed, and accepted by the Associate Vice Chancellor for Campus Operations or designee.

D. The Facilities Technology Support Manager shall maintain a database of all shared user accounts in the Keepass database.

E. The Facilities Technology Support Manager shall assist Facilities Services with in-kind replacement of devices and shall update Infoblox and Keeppass to reflect changes to device information and access privileges.

F. Privilege access to critical University systems shall be assigned based on job role and responsibilities and documented. Procedures shall be established and maintained to avoid the unauthorized use of generic administration user IDs.

G. Default product or vendor account passphrases shall be secured and, wherever possible, changed to prevent unauthorized access. Product or vendor accounts no longer needed shall be disabled to prevent unauthorized access.

H. Facilities Services Supervisors in collaboration with the Facilities Technology Support Manager shall review all critical University systems to ensure users' access rights, including privileged access rights, are adjusted appropriately and in a timely manner whenever there is a change in University needs; in response to changes in risk(s) affecting the reliability, integrity, or availability of the system(s); whenever a user's job role or responsibilities change; or a user separates from the University.

I. Users' access rights to critical University systems shall be reviewed no less than annually. The annual review shall be initiated by an annual preventative maintenance work order. Any changes to access rights or audit findings shall be entered into the CMMS.

J. Users' access rights to critical systems shall be revoked in a timely manner based on risk(s) to the University. In the unforeseen case where a user's access rights cannot be revoked upon employment separation, Facilities Services Department Heads in collaboration with the Facilities Technology Support Manager must consider whether the continued system access rights constitute an unacceptable risk to the University and, if so, revoke the user's access rights or request a risk acceptance.

K. User activities, including those performed with privilege access, within critical University systems shall be monitored by Facilities Services Supervisors to determine risk(s) to the University and to identify potential misuse of systems.

L. Reviews logs for critical University systems shall be:
a) Protected from unauthorized access, modification, loss, or destruction.
b) Regularly reviewed based on risk to the University to identify security concerns in need of attention, investigation, and, if necessary, corrective action.
c) Retained until the University determines the information is no longer valuable or as required by legal and regulatory requirements.

V. NETWORKED DEVICES

A. Facilities Services Networked Device Summary

1. Facilities Services operates and maintains a large array of networked devices. Technology is rapidly changing and with these changes brings enhancements to the devices used every day to keep University community safe and comfortable. A listing of the general categories and a brief description of the systems is as follows:

   a. Building Automation System (BAS) – A complex system of multi-tiered devices that control, monitor, report and alarm related to the University Heating, Ventilation and Air Conditioning (HVAC) system. This includes HVAC equipment such as Air Handling Unit (AHU), pumps, chillers, and fans. The BAS can include servers, building level controllers, and equipment level controllers. Most of these systems are monitored 24/7 by Facilities Services or at a minimum daily.

   b. Fire Alarm System (FAS) - A complex system of multi-tiered devices and controls that provide monitoring, reporting and alarming for the detection and evacuation of a fire (smoke or heat). The components that make up the FAS include fire alarm control panels, sub panels, smoke/heat detectors, dialers, and audiovisual alarms. The networked devices can include servers, workstations, and Fire Alarm Control Panel (FACP) dialers. These systems may also interface with other systems such as a BAS to shutdown HVAC equipment during a fire or close fire dampers.

c. Enterprise Utility Data Acquisition System – A complex system of multi-tiered devices that provide monitoring, reporting, and alarming of building utilities (electricity, natural gas, and water). The system includes a server (VM), meters, and communication bridges. The data collected from this system enables Facilities Services to understand the energy usage of University's facilities. This system does not provide control of any devices, only monitors.

d. Water Treatment Systems - A system of multi-tiered devices that monitor water chemistry in cooling towers and closed loops of HVAC hydronic systems and injects chemicals to maintain water chemistry within desired control limits to prevent corrosion of system components or the growth of biological organisms. The water treatment system networked devices can include desktop computers for storing historical data and chemical controllers.

e. Medical Gas and Vacuum Systems - A system of multi-tiered devices that monitor and alarm related to the function of centralized medical gas and vacuum systems. These systems include master panels, area panels, and compressed gas manifolds. These systems are located in both patient care areas such as located in the School of Dental Medicine and research areas such as located in the vivariums.

f. Lighting Control Systems - A system of multi-tiered devices that allow for the centralized scheduling and control of lighting systems. These systems can include a PC or controller for adjusting schedules as well as field devices that actual turn the lights on and off. These systems may be used to reduce energy usage by coordinating occupied periods with University schedules or in research areas where specific lighting cycles are required.