SOP FOR IT FACILITIES

1. Purpose

The goal is to offer Centurion University staff members and system users high-quality technical services by the university's information technology Team, as well as to help computer users find the right source to address their inquiries, fix any network- or computer-related issues, update in-house applications, assist with particular team needs, and aid them in finding appropriate computer-related resources

2. Mission Statement

The information technology team's goal is to offer chances for improving and enhancing Centurion University operations via the application and incorporation of technological breakthroughs in hardware and software.

3. Organizational Description/Scope of Work

The Centurion University computer network, software and hardware inventory, telecommunications network, and other technology are all maintained and overseen by the IT Team, which also offers technical help. The Centurion University IT Team invites all departments to collaborate so as to plan for the institution's future computer environment. Additionally, we believe that by being aware of the crucial role the IT Team plays in preserving the dependability and integrity of computer resources, our staff will work with us to develop Centurion University's future computing environments.

4. Responsibility and Role of the IT Team

The IT team chooses and conceptually plans the finest technological solutions to achieve the team's and Centurion University's aims. Systems will be installed, maintained, and upgraded as needed by the IT team. The IT staff will be in charge of conducting research and creating fresh approaches to complete jobs quickly and effectively. The network as a whole is impacted by every computer and team that is introduced to the Centurion University servers. The ability of the IT Team to adequately handle new devices and apps frequently necessitates the addition of additional resources, the installation of which may take some time. As required, the IT Team will balance the workload of services among resources. Including the IT Team in early talks enables team to begin making plans to support and maintain

a. PBX's & Voice Mail Systems
b. Internet Access & E-mail
c. Computer/Laptop Hardware
d. Program Software
e. Copiers/Fax/Scanners- All peripherals
f. Video and Audio equipment
g. Maintain network security and performance; establish workable directory structure, network security, and disk space allocation, etc.
h. Set up user accounts according to set established policies, procedures, and limitations.
i. Track all problems or issues through work orders.
j. Plan new phone lines and data ports when needed.
k. Perform network maintenance, changes, and upgrades.
l. Enhance network by assessing new software and hardware products that would increase network performance and expand network services.
m. Direct the performance of regularly scheduled systems management and maintenance procedures designed to ensure the integrity of all programs by running backup procedures and diagnostic software routines.
n. Implement disaster recovery plans; runs system backups and disaster recovery operations.
o. Develop procedural documentation or policies as needed.
p. Provide technical advice and training to Centurion University operations staff in the operation, maintenance, and support of computer hardware and software system.
q. Train and update staff with respect to security systems.
r. Prepare reports and makes recommendation to ensure the optimum efficiency of equipment and systems in accordance with departmental needs.
s. Maintain stock of expendable and non-expendable computer equipment, materials, system, application, and supplies sufficient to ensure continuous and uninterrupted operation of systems; communicates with vendors regarding purchases.
t. Maintain professional and technical knowledge by conduction research; attending seminars, education workshops, classes and conferences; reviewing professional publications; establishing agencies and related organizations.
u. CCTV's have been placed in all the corridors, lobbies, auditorium, AV rooms, all labs, library, digital,waiting rooms, hostels, canteens, mess, kitchen and at places that are commonly accessed by stakeholders.
v. The CCTV surveillance system would track and prevent the entry of anti-social elements and ensure safety & security to all the stakeholders (staff, students, faculty, parents, visitors, etc) and facilities of the campus.

5. Software

The IT team is responsible for maintaining all software on the systems. The following processes will be followed with regard to software:

a. The IT Team will maintain a current list of standard and recommended software.
b. To ensure software is compatible and not destructive to the CUTM computer systems, the IT Team will approve any and all software programs.
c. If a user is interested in software that is not on the maintained list, the user will need to complete an IT Work Order to request assistance in determining if that software is sustainable on CUTM computer systems and network.
d. The IT Program will determine if software is qualified as being compatible with CUTM's system.
e. If software is not qualified as being compatible with the CUTM's standard software or the CUTM system, software cannot be installed on the system.
f. If a software program exceeds the specifications of the user's computer system, the user will be notified to look for alternative software or to find program funds to upgrade the system.
g. All software installed on Centurion University of computers or on the servers must have a valid license.
h. Should sever-based software make a server unstable, the IT Team will be responsible for restoring any data that was stored on a server that is backed up by the IT Team's backup server.
i. The IT Team is obligated by certain software vendors to monitor all software licenses in order to ensure compliance with the vendor's license agreements.
j. Users may contact the IT Team to obtain additional guidance, quotes and advice on any software.
k. Types of Software used at the Centurion University of:

   i. Standard software is that software (open source and licensed) which is made available to users by the Centurion University and maintained by the IT Team. The IT Team installs all software, and may upgrade it when new releases become available. If training is required for newly purchased software a work order must follow request.

   ii. Departmental funded software is software that is used by one or more departments or teams that are specific to that particular program. All departmental software must maintain a valid license for such software.

iii. Individual funded software is approved software that a single user purchases for which they have a valid license and deems important to his or her departments success. User must submit a work order if installation of individual funded software on their local workstation's hard drive is needed. To demonstrate legality of the software, the user must be able to produce the original installation of diskettes/cds and license at any time. If any installed software somehow makes a computer unstable, the IT Team will remove the software and restore local station back to the standard configuration.

The University does not encourage the use of pirated software.

6. Hardware

The IT team is responsible for maintaining all software on the systems at Centurion University. The following processes will be followed with regard to software.

a. The IT Team will maintain a current list of standard and recommended hardware.
b. To ensure hardware is compatible and not destructive to the CUTM's computer systems, the IT Team will approve any and all hardware programs.
c. If a user is interested in hardware that is not on the maintained list, the user will need to complete an IT Work Order requesting assistance in determining if that software is sustainable on CUTM computer systems and network.
d. The IT team will determine if hardware is qualified as being compatible with CUTM's systems.
e. If hardware is not qualified as being compatible with the CUTM's standard software or the CUTM systems, it will not be installed.
f. The IT Team will be responsible for all hardware that is associated with the CUTM Servers.
g. Types of common hardware used at the Centurion University of
h. Fully supported hardware are those hardware devices which are maintained by the IT Team. The IT Team recommends installs and tests for compatibility of such hardware with all supported environments, and may upgrade hardware when new drivers are released or become available.

7. Application Hosted @ Amazon EC2

Security:
Manage access to AWS resources and APIs using identity federation, IAM users, and IAM roles. Establish credential management policies and procedures for creating, distributing, rotating, and revoking AWS access credentials

Implement the least permissive rules for your security group.

Regularly patch, update, and secure the operating system and applications on your instance.

Use Amazon Inspector to automatically discover and scan Amazon EC2 instances for software vulnerabilities and unintended network exposure.

Storage
Understand the implications of the root device type for data persistence, backup, and recovery.

Use separate Amazon EBS volumes for the operating system versus your data. Ensure that the volume with your data persists after instance termination.

Use the instance store available for your instance to store temporary data. Remember that the data stored in the instance store is deleted when you stop, hibernate, or terminate your instance. If you use instance store for database storage, ensure that you have a cluster with a replication factor that ensures fault tolerance.

Encrypt EBS volumes and snapshots

Resource management
Use instance metadata and custom resource tags to track and identify your AWS resources.

View your current limits for Amazon EC2. Plan to request any limit increases in advance of the time that you'll need them.

Use AWS Trusted Advisor to inspect your AWS environment, and then make recommendations when opportunities exist to save money, improve system availability and performance, or help close security gaps.

Backup and recovery
Regularly back up your EBS volumes using Amazon EBS snapshots, and create an Amazon Machine Image (AMI) from your instance to save the configuration as a template for launching future instances. For more information on AWS services that help achieve this use case, see AWS Backup and Amazon Data Lifecycle Manager.

Deploy critical components of your application across multiple Availability Zones, and replicate your data appropriately.

Design your applications to handle dynamic IP addressing when your instance restarts.

Monitor and respond to events.

Ensure that you are prepared to handle failover. For a basic solution, you can manually attach a network interface or Elastic IP address to a replacement instance. For an automated solution, you can use Amazon EC2 Auto Scaling.

Regularly test the process of recovering your instances and Amazon EBS volumes to ensure data and services are restored successfully.

Networking

Set the time-to-live (TTL) value for your applications to 255, for IPv4 and IPv6. If you use a smaller value, there is a risk that the TTL will expire while application traffic is in transit, causing reachability issues for your instances.

8. Campus Networking

- Router configuration files shall be secured by providing access rights given by Network Administrator only to authorized users.
- An external firewall maintained by Network Administrator shall separate CUTM network from the external untrusted networks. Servers facing the public network shall be in DMZ
- Network architecture shall be such that each application and database server of production environment shall be in clustering mode and proper backup shall be scheduled periodically.
- Network components used for network security shall be configured properly and quarterly tested by Network Administrator. The backup of these configurations shall be taken quarterly or when any changes made to the system.
- Documentation related to Network devices, configuration and architecture shall be properly maintained and updated when required.
- Appropriate tools shall be deployed to manage and monitor network health on daily basis. Proper log shall also be maintained which specify type of network, bandwidth limits, inbound & outbound traffic etc. and can archived for future reference.
- Access control lists must be used to limit the source and type of traffic that can terminate on the device itself. Wherever technically feasible, single points of failure in network shall be minimized.
- The Network Administrator shall evaluate each new release of the network component to determine whether any upgrade is required or not.
- Password, Firewall, Antivirus, Remote Access and logical access control Policy shall be followed strictly to access the network devices / services.
- IPS shall be configured to ensure detection and prevention of any malicious network traffic entering the network. Network shall be restricted and secured through firewall, web content filtering and Intrusion Detection System.
- Network devices shall be configured to display logon banners which provide adequate warning against unauthorized logon attempts. These banners shall give least information about the network and system to the user.

- Before using your wireless router, turn on security. Use WPA security and not WEP. Wi-Fi configuration will be defined on the firewall to bind user login with MAC address of user. Place the router in a physically secure place.

9. Prohibited hardware and software

The following hardware and software are not permitted, and the IT team will monitor their installation on Centurion University systems:

a. Hardware or software that makes any portion of the network unstable.
b. Hardware or software that is used for illegal purposes
c. Hardware of software which there are licensing issues which legally prohibit its use.
d. Hardware or software may also be prohibited due to its tendency to destabilize or compromise the security of core network services.

Any hardware or software that causes any part of the network to become unstable will always be instantly removed from the network, and the system will then be reset to its default settings.

10. Portable Devices

The users of portable devices are responsible for such devices and will be held accountable for the care of such devices. The term "portable device" includes but is not limited to the following:

a) Laptops
b) External hard disk drives
c) USB data devices
d) Portable music players
e) Storage media – CD/DVD/SD/mini SD/memory sticks
f) iPads
g) Mobile phones – basic and smartphones
h) Data access points – MiFi cards

When not in use, these devices must be stored appropriately and have updated, certified antivirus software installed (if applicable). Prior to receiving a portable device, all users must obtain the right authorization from their supervisor. The IT Team will keep track of all devices that have been issued and will keep an eye on how they are being used.

11. Replacement Plan

The Centurion University will pursue a four-year plan for replacing its computers. Using this strategy, it will be possible to replace outdated computers that are now connected to the Centurion University of Network but are:

a. Not adequate to provide access to all services available on the Centurion University's network or
b. Not adequate to support advanced needs of the specific user.

An IT Work Order with a request for a quote and a thorough rationale for why the computer must be replaced must be provided to the IT Team if a system needs to be upgraded before the scheduled computer replacement date.

12. Relocation of Computers or Printers

All computer systems and accessories which has to be moved, will be the responsibility of the IT team. To prevent delays in the setup procedure, an IT Work Order is to be sent to the IT Support email address at least five business days before the relocation. The user must get in touch with the IT Manager in the event of a serious emergency.

13. Equipment to be Checked Out

All IT equipment is maintained by the IT team. By filling out an IT Work Order, you can check out this equipment (laptops, digital cameras). Only materials needed for Centurion University business may be checked out. It is crucial for the user to abide by all applicable laws and regulations when using the equipment. Users are prohibited from recording content that violates copyright laws when using the CUTM camera without the copyright holder's consent. Taking pictures with a camera or another device at concerts, exhibitions, or commercial premises may violate copyright or other legal rights, even if the picture was taken for commercial purposes.

14. Website

The Centurion University website is made to give access to outsiders to details about the institution, its activities, and entity. The CUTM Website is subject to the following:

a) Departments / Teams are responsible for ensuring their webpage is updated at least every 30 days.
b) All content submitted for posting on the website must state a source. All external sources will be credited.
c) Copyrighted material must be accompanied by a properly executed release from the author and/or photographer.
d) Copies of properly executed release forms are required when posting photos of minors and non-users.
e) The website calendar is provided for University events only.
f) Links to websites found to be under construction or inactive will be removed. No links to personal websites will be posted.

Centurion University

15. Disposal of Electronic Equipment

The IT team gets rid of old electronic devices. The user must fill out an IT Work Order and email it to the IT Support email address in order for the IT Team to dispose of the device. The IT Team will store out-of-date equipment for at least 60 days before disposing of it at an environmentally friendly electronics recycling facility. There, the hard drives will be destroyed and a certificate of destruction will be issued when the equipment is recycled.

16. Data Backup/Disaster Recovery Plan

The Centurion University's servers, which are spread across several sites, are fully automated backup services provided by the IT team. Data backups are created only to help with disaster recovery, not to store them for later retrieval. The Catastrophe Recovery Plan for Centurion University details the steps taken by the IT team for technology disaster recovery as well as the stages of the process for retrieving important data. The plan for the IT Team ensures that operations may be quickly and successfully recovered and minimizes interruptions to crucial processes.

17. Maintenance

The IT Team will plan quarterly network maintenance to upgrade the hardware and software and check for problems.

18. Security

The IT Manager is in charge of data security. A top goal of the IT Team is the security of the computer system at Centurion University. The following are elements of the security monitoring process used by the IT Team:

a) Each Department and Team will determine what data is considered public, confidential, or for official use only.
b) The IT Manager will review all security alerts.
c) The IT Manager will setup logs and review them to monitor possible security breaches.
d) The IT Manager must maintain backups as needed to recover from deliberate security threats and damage.
e) The IT Team will use email security software to protect the Centurion University's network from email threats in the form of viruses and SPAM.
f) The IT Team staff will log onto the email appliance to monitor mail activity with the intent of detecting email threats.
g) The IT Team is able to log on to the server remotely to ensure the network's security is effective.
h) The CUTM network is equipped with a firewall to secure encrypted tunnel for remote users to gain a secure connection from outside the network.

i) The CUTM network is equipped with content filtering which allows for control of the users Internet access to the web. This service is used to monitor user's website visits and block inappropriate websites.

j) If a user suspects security violation, they should submit an IT Work Order to the IT Support email address detailing the time and error that occurred on the user's system.

19. Remote Access

Only safe, authenticated, and centrally managed access methods are allowed for remote access to the Centurion University's computer network and data. This access can only be used to conduct Centurion University business and needs to be authorized by the user's supervisor. The IT Manager will set up a VPN connection and make sure it is secured and verified.

20. User Accounts, Email & Passwords

All CUTM email addresses and accounts are assigned updates, and the IT team keeps track of them. The IT Team also keeps track of and upgrades all system passwords as necessary for every individual user. At the time of hire, every new employee whose work necessitates the use of a computer will be given an email address with a password. Each supervisor must submit the proper IT Work Order to the IT Team in order to request the setup of a new user account. Every six months, all computer users must change their passwords. Each user's PC will automatically prompt them to update their passwords. If the system has been compromised, the IT Team reserves the right to demand that users change their passwords immediately.

21. Internet Access

The internet gives users access to a wide range of information, some of which may be valuable and some of which may not, and it is not a safe way to communicate. The user is in charge of making sure that the Computer, Intranet, and Internet Use Policy of Centurion University is adhered to. Through monitoring and filtering software, the IT Team will keep an eye on user activities to block access to websites that are forbidden or in violation of CUTM regulations.

22. Teleconferencing / Audio Visual

All departments and team will receive support from the IT team for any teleconference or audio visual requirements. The following needs to happen for a conference or presentation to be successful:

a) An IT Work Order must be received by the IT Team at least 24 hours in advance to ensure adequate staffing is available for the request.

b) Requests for teleconferencing that require more than 3 lines to be teleconferenced into a Centurion University telephone line require at least five (5) business days advance notice.

c) The IT Team will call the Work Order initiator to ensure the details of the project and plan accordingly.

d) Detailed instructions for the teleconferencing systems in the Centurion University Council Chambers and at the Public Works Conference room are available at each location.

23. Telephones / Communications

All landlines and mobile phones are managed and watched over by the IT team. The user's supervisor must first provide their approval before using any telephone lines, long distance codes, data cards, or mobile phones. The supervisor will utilize an IT Work Order to submit the request to the IT Manager to install or add a line for a user.

24. Quote Requests

An IT Work Order must be sent to the IT Support email address if a quote is needed for any software or peripherals. The Work Order must provide a thorough description of the user's required specifications.

25. Problem Resolution

The CUTM network's users, including staff members and other users, are the focus of the IT Team's efforts to deliver the most effective and efficient services. If there is an issue with the IT Team's services or personnel for whatever reason, the team should be contacted. The complainant should go directly through the proper chain of command if this does not result in an improvement.

26. Reporting

Every quarter or as needed, the IT Team must give the Administrative Services Director a progress report. The annual schedule for the CUTM Annual Report and the annual budget narratives is established. The IT Team personnel is in charge of making sure all deadlines are reached in accordance with instructions.

27. IT Work Order

A user must fill out an IT Work Order and send it to the IT Support email address or using ERP HelpDesk, if they are having issues with their computer system or another electronic device. In case of an emergency or if email/internet isn't working. The appropriate solution will be chosen based on how serious the issue is. There are occasions when a problem affects the entire department or company. The IT team will need to conduct additional study on these issues, and they frequently need to coordinate solutions with outside parties.