Network Infrastructure Proposal

COSCare

May 15, 2020

Report by:

Jacob Metcalfe

Table of Contents

Policies

Audit Policy

1.0 Purpose
To provide guidelines for employees to follow about the network scanning policies at COS Care the IT department will be responsible for performing all electronic scans of networks, firewalls, and systems utilizing Intelex software.

Audits may be conducted to:

- Ensure integrity, confidentiality, and availability of information and resources
- Investigate possible security incidents ensure conformance to COS Care security policies
- Investigate security incidents recorded in security logbook
- Monitor user or system activity where appropriate.

2.0 Scope
This policy covers all computer and communication devices owned or operated by COS Care agents and subsidiaries. This policy also covers any computer and communications device that are present on COS Care premises, but which may not be owned or operated by COS Care (This means your phones and tablets are subject to scans). The IT department can perform Denial of Service activities; however, these activities will not affect the hospitals performance.

3.0 Policy
By accepting the offer for employment at COS Care all employees consent to access by members of the IT dept.

This access may include:

- User level and/or system level access to any computing or communications device
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on COS Care equipment or premises.
- Access to work areas (labs, offices, nurse stations, storage areas, etc.)
- Access to interactively monitor and log traffic on COS Care networks.

All system logs are monitored using Splunk and is stored in the System Log Database.

3.1 Service Degradation and/or Interruption. Network performance and/or availability may be affected by the network scanning. The IT department will send out multiple warnings to prepare staff for slowdowns. If interruptions occur and there was no warning from either the IT department or your system administrator, please contact your system administrator to ensure services are working as intended.

3.2 Scanning period. The IT department's Scanning Team shall identify in writing the allowable dates for the scan to take place with a maximum of a week notice.

3.3 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Acceptable Use Policy (AUP)

1.0 Purpose

The purpose of this policy is to establish a standard for rules and responsibilities when connected to the COSCare network.

2.0 Scope

The scope of this policy includes all employees who have any type of access to the COSCare network, and any employee responsible for overlooking the COSCare guest network.

3.0 Policy

Prior to working on a COSCare workstation, every employee must sign an Acceptable Use Policy (AUP). The AUP is to contain a set of rules established by the IT Department that sets guidelines as to how the system is to be used. Guidelines directly follow the SANS Institute, in which is well known for their security training and their widely accepted guidelines to be followed. These guidelines are referenced at: https://www.sans.org/security-resources/policies/general/pdf/acceptable-use-policy.

3.1 General Use and Ownership
- COS Care proprietary information stored on electronic and computing devices remains the sole property of COS Care. This policy remains in effect for leased systems as well.
- Proprietary information is to be protected in accordance with the Data Protection Standard
- Every Employee has a responsibility to promptly report theft, or loss of COS Care proprietary information.
- You may access, use, or share COS Care information only to the extent it is authorized and necessary to fulfill your assigned job duty.
- Individual departments are responsible for creating guidelines concerning personal use of Internet systems.
- In times of uncertainty, employees are to consult their supervisor or manager.
- COS Care may monitor equipment, systems, and network traffic at any time per COS Care's Audit Policy.
- COS Care reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

3.2 Security and Proprietary Information
- System level and user level passwords are to comply with the technical group policy.
- Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

- Postings to any newsgroup by employees from a COS Care email address should contain a disclaimer if opinions are involved stating that those opinions are strictly their own and not necessarily those of COS Care.
- Employees are to use extreme caution when opening any emails with attachments.

3.3 Unacceptable Use

The following activities are strictly prohibited unless written job responsibilities state otherwise. No Employee of COS Care is authorized to engage in any illegal activity under local, state, federal, or international law while utilizing COS Care resources.

- Violations to rights of any person or company protected by copyright, patent, or intellectual property, including pirated material.
- Unauthorized copying of copyright material.
- Accessing data, a server or account for any purpose other than conducting COS Care business.
- Exporting software, technical information, or software.
- Introduction of malicious programs into the network or server.
- Revealing account password.
- Transmitting material in violation of sexual harassment or hostile workplace laws.
- Making fraudulent offers of products, items, or services.
- Making statements about warranty.
- Port or security scanning.
- Executing any form of network monitoring.
- Circumventing user authentication or security of any host, network, or account.
- Introducing honeypots, etc. onto any COS Care network.
- Interfering with or denying service to any user/system.
- Using any program/script to interfere with or disable a user's terminal session.
- Providing information about, or lists of, COS Care employees to parties outside of COS Care.

Backup Policy

1.0 Purpose

This policy is designed to protect data in the hospital to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

2.0 Scope

This policy applies to all equipment and data owned and operated by COS Care.

3.0 Definitions

3.1. Backup - The saving of files onto dedicated backup server or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.

3.2. Archive - The saving of old or unused files onto the dedicated backup server or other offline mass storage media for the purpose of releasing on-line storage room.

3.3. Restore - The process of bringing offline storage data back from the offline media and putting it on an online storage system such as a file server.

4.0 Timing
Incremental backups performed daily at midnight and full backups are performed weekly on Friday at 11:59pm. If for maintenance reasons backups are not performed on Friday, then they shall be done on Saturday or Sunday.

5.0 Responsibility
The IT department manager shall delegate a member of the IT department to develop a procedure for testing backups and test the ability to restore data from backups on a monthly basis.

6.0 Required Backups
Data to be backed up include the following information:

1. User data stored on the hard drive.
2. System state data
3. The registry
4. All patient data stored on the user's machine and devices

Systems to be backed up include but are not limited to:

1. File server
2. Mail server
3. Production web server
4. Production database server
5. Domain controllers
6. Test database server
7. Test web server
8. Closed patience record database
9. Active patience record database

8.0 Archives
Archives are made at the end of every quarter with manual archival requests possible. User account data associated with the file and mail servers are archived two weeks after they have left the organization.

9.0 File Restoration
Users that need files restored must submit a request to the help desk. Include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

10.0 Dedicated Backup Server Location
The server used for weekly backups shall be stored in an offsite building in an undisclosed location. An additional Archive server shall be stored in the basement of the hospital along with the trolls that guard it.

Captive Portal Policy

1.0 Purpose
The purpose of this policy is to establish a standard for all devices and their activity connecting to the COSCare guest network.

2.0 Scope
The scope of this policy includes all individuals who enter the guest network and sign the captive portal agreement.

3.0 Policy
3.1 General

- All systems are to be verified before entering the DMZ of the guest network
- All systems are required to sign a web page that uses multifactor authentication for sign on in the guest network.
- Multifactor authentication will be both digital signature and verifying email to ensure health information safety.
- This guest network is to adhere to all other policies when additions to the guest network are necessary.
- All IT Admins are to adhere to group policy standards even on the guest network
- Users on the guest network will not be available to download anything while on the network, nor will they be able to save anything to the SSD/Hard drive of a workstation.
- Cookies and all browser data will not be stored on the system.
- All information will be logged into the Splunk database to ensure health information safety.
- Permissions will limit the user to only browsing the internet, streaming services, and mobile games.

3.2 Guidelines

- All guidelines are referenced from sites.google.com/site/wifitermsgeneric/
- Any additional guidelines can be appended below.
  The following is what the user will see upon connecting to the COSCare guest Wifi.

Captive Portal Form
3.3 Terms and Conditions
By connecting to COSCare-Guest internet service, you herby acknowledge and agree that there are significant security, privacy, and confidentiality risks inherent in accessing or transmitting information through the interne, where the connection is facilitated though wired or wireless connection. Security hazards include transmission interception, potential malware, hacking, loss of data, or potential damage to your connecting system.
Accordingly, by signing this form you agree that COSCare is not liable for any of the above listed security hazards that result from the connection of this provided internet service.
Use of this wireless network is subject to the general restrictions outlined below. If abnormal, illegal, or unauthorized behavior is detected the network provider reserves the right to

permanently disconnect the offending device from the network and pursue any further legal actions necessary.

3.3 Examples of Illegal Uses

The following are representative examples only and do not comprise a comprehensive list of illegal uses:

1. Spamming and invasion of privacy - Sending of unsolicited bulk and/or commercial messages over the Internet using the Service or using the Service for activities that invade another's privacy.
2. Intellectual property right violations - Engaging in any activity that infringes or misappropriates the intellectual property rights of others, including patents, copyrights, trademarks, service marks, trade secrets, or any other proprietary right of any third party.
3. Accessing illegally or without authorization computers, accounts, equipment or networks belonging to another party, or attempting to penetrate/circumvent security measures of another system. This includes any activity that may be used as a precursor to an attempted system penetration, including, but not limited to, port scans, stealth scans, or other information gathering activity.
4. The transfer of technology, software, or other materials in violation of applicable export laws and regulations.
5. Export Control Violations
6. Using the Service in violation of applicable law and regulation, including, but not limited to, advertising, transmitting, or otherwise making available ponzi schemes, pyramid schemes, fraudulently charging credit cards, pirating software, or making fraudulent offers to sell or buy products, items, or services.
7. Uttering threats.
8. Distribution of pornographic materials to minors.
9. Child pornography.

3.4 Examples of Unacceptable Uses

The following are representative examples only and do not comprise a comprehensive list of unacceptable uses:

1. High bandwidth operations, such as large file transfers and media sharing with peer-to-peer programs (i.e. Torrents)
2. Obscene or indecent speech or materials
3. Defamatory or abusive language
4. Using the Service to transmit, post, upload, or otherwise making available defamatory, harassing, abusive, or threatening material or language that encourages bodily harm, destruction of property or harasses another.
5. Forging or misrepresenting message headers, whether in whole or in part, to mask the originator of the message.
6. Facilitating a Violation of these Terms of Use
7. Hacking
8. Distribution of Internet viruses, Trojan horses, or other destructive activities
9. Distributing information regarding the creation of and sending Internet viruses, worms, Trojan horses, pinging, flooding, mail-bombing, or denial of service attacks. Also, activities

that disrupt the use of or interfere with the ability of others to effectively use the node or any connected network, system, service, or equipment.
10. Advertising, transmitting, or otherwise making available any software product, product, or service that is designed to violate these Terms of Use, which includes the facilitation of the means to spam, initiation of pinging, flooding, mail-bombing, denial of service attacks, and piracy of software.
11. The sale, transfer, or rental of the Service to customers, clients or other third parties, either directly or as part of a service or product created for resale.
12. Seeking information on passwords or data belonging to another user.
13. Making unauthorized copies of proprietary software or offering unauthorized copies of proprietary software to others.
14. Intercepting or examining the content of messages, files, or communications in transit on a data network.

3.5 Digital Signature and Email Verification (Multifactor Authentication)
User is asked to sign their name and enter their email address to allow access to the guest network. Signing this form means that you accept all terms and conditions as stated above. Failure to do so, will discontinue network access.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Any public user found to have violated this policy will be immediately reported to the authority deemed necessary.

Database Password Policy

1.0 Purpose
The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

2.0 Scope
The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any COS Care facility, has access to the COS Care network, or stores any non-public COS Care information.

3.0 Policy
3.1 General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All production system-level passwords must be part of the InfoSec administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.

- Passwords must not be inserted into email messages or other forms of electronic communication.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.

3.2 Guidelines

A. General Password Construction Guidelines

Everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics (What not to do):

- The password contains less than fifteen characters (can be cracked easily with openly available software i.e., Jack the Ripper, etc...)
- The password is a word found in a dictionary (English or foreign, the first thing they check)
- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, imaginary girlfriends, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - Including the words "COS Care", "Colorado", "Springs" or any derivation.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret, or secre1)

Strong passwords have the following characteristics:

- Minimum of nine characters
- Contain both upper- and lower-case characters (e.g., a-z, A-Z) at least one of each
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least fifteen alphanumeric characters long and is a passphrase (TheHeartSh0uldn’tBeThere00ps).
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way to Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards

1. Do not use the same password for COS Care accounts as for other non-COS Care access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, do not use the same password for various COS Care access needs (for the few of you that have diversified access permissions). For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.
2. Do not share COS Care passwords with ***anyone***, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential COS Care information.

Here is a list of " Do not's ":

- Do not reveal a password over the phone to **ANYONE**
- Do not reveal a password in an email message
- Do not reveal a password to your supervisor
- Do not talk about a password in front of others
- Do not hint at the format of a password (e.g., "my family name")
- Do not reveal a password on questionnaires or security forms
- Do not share a password with family members
- Do not reveal a password to co-workers while on vacation
- Do not reveal a password to a patient under anesthesia even if they promise not to tell

3. If someone demands a password, refer them to this document or have them call someone in the IT Department.
4. Do not use the "Remember Password" feature of applications (e.g., Eudora, OutLook, Messenger).
5. Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption (use common sense).
6. Your password will expire every six months (except system-level passwords which will expire quarterly). The recommended change interval is every four months.
7. If an account or password is suspected to have been compromised, report the incident to the IT department and change all passwords.
8. If you forget your password and get locked out, contact IT and after you are verified, they will reset the password for you. Then you will be required to set a new password that adheres to this password policy.
9. Password cracking or guessing may be performed on a periodic or random basis by the IT department or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it and buy lunch for everyone in the IT department.

C. Application Development Standards
Application developers must ensure their programs contain the following security precautions.

Applications:

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

- should support TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

D. Use of Passwords and Passphrases for Remote Access Users
Access to the COS Care Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

E. Passphrases
Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.
Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."
A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:
"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"
All of the rules above that apply to passwords apply to passphrases.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions
Terms Definitions
Application Administration Account Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).

Disaster Recovery Policy

A disaster recovery team shall be appointed with members from IT, and the executive staff and will be reviewed annually for relevance. The disaster recovery team will perform the following duties:

- Perform an initial risk assessment to determine current information systems vulnerabilities.
- Perform an initial business impact analysis to document and understand the interdependencies among business processes and determine how the hospital would be affected by an information systems outage.
- Take an inventory of information systems assets such as computer hardware, software, applications, and patient data.
- Identify critical applications, systems, and data.
- Prioritize key hospital functions.
- Conduct simulated disasters to test effectiveness of policies and capabilities of the disaster recovery team.

Hospital personnel will carry out the following procedures in the implementation of a disaster recovery policy.

- Document and distribute the recovery plan to all staff of the hospital.

- Distribute copies of the written plans to everyone involved and store extra copies in an offsite, fireproof vault.
- The following are ongoing procedures that must be followed:
    - Continuously perform data backups, store at least weekly backups offsite, and test those backups regularly for data integrity and reliability.
    - Test plans at least annually, document and review the results, and update the plans as needed.
    - Analyze plans on an ongoing basis to ensure alignment with current business objectives and requirements.
    - Provide security awareness and disaster recovery education for all team members involved.
    - Continuously update information security policies and network diagrams.
    - Secure critical applications and data by patching known vulnerabilities with the latest fixes or software updates.

Acknowledging Receipt of Disaster Recovery Policy

I have received my copy of the COS Care Disaster Recovery Policy and I have read and understand the information contained herein.
I further acknowledge my understanding that my employment with COS Care may be terminated at any time with or without cause.

_____

Head of IT SignatureDate

_____

Name [Please Print]

_____

Employee's Signature

DMZ Internet Policy

1.0 Purpose

The purpose of this policy is to define standards to be met by all equipment owned and/or operated by COS Care located outside COS Care corporate Internet firewalls. These standards are designed to minimize the potential exposure to COS Care from the loss of sensitive or hospital-deemed confidential data (i.e. patient files), intellectual property, damage to public image etc., which may follow from unauthorized use of COS Care resources.
Devices that are Internet facing and outside the COS Care firewall are considered part of the "demilitarized zone" (DMZ) and are subject to this policy. These devices (network and host) are particularly vulnerable to attack from the Internet since they reside outside the corporate firewalls.

The policy defines the following standards:

- Ownership responsibility
- Secure configuration requirements
- Operational requirements
- Change control requirement

2.0 Scope

All equipment or devices deployed in a DMZ owned and/or operated by COS Care (including hosts, routers, switches, etc.) and/or registered in any Domain Name System (DNS) domain owned by COS Care, must follow this policy.

This policy also covers any host device outsourced or hosted at external/third-party service providers if that equipment resides in the "COSCare.com" domain or appears to be owned by COS Care.

All new equipment which falls under the scope of this policy must be configured according to the referenced configuration documents unless a waiver is obtained from InfoSec. All existing and future equipment deployed on COS Care's un-trusted networks must comply with this policy.

3.0 Policy

3.1. Ownership and Responsibilities

Equipment and applications within the scope of this policy must be administered by support groups approved by InfoSec for DMZ system, application, and/or network management.

Support groups will be responsible for the following:

- Equipment must be documented in the hospital-wide enterprise management system. At a minimum, the following information is required:
  - Host contacts and location.
  - Hardware and operating system/version.
  - Main functions and applications.
  - Password groups for privileged passwords.
- Network interfaces must have appropriate Domain Name Server records (minimum of A and PTR records).
- Password groups must be maintained in accordance with the corporate wide password management system/process.
- Immediate access to equipment and system logs must be granted to members of InfoSec upon demand, per the *Audit Policy*.
- Changes to existing equipment and deployment of new equipment must follow and corporate governess or change management processes/procedures.

To verify compliance with this policy, InfoSec will periodically audit DMZ equipment per the *Audit Policy*.

3.2. General Configuration Policy

All equipment must comply with the following configuration policy:

- Hardware, operating systems, services and applications must be approved by InfoSec as part of the pre-deployment review phase.
- Operating system configuration must be done according to the secure host and router installation and configuration standards.
- All patches/hot fixes recommended by the equipment vendor and InfoSec must be installed. This applies to all services installed, even though those services may be temporarily or permanently disabled. Administrative owner groups must have processes in place to stay current on appropriate patches/hotfixes.

• Services and applications not serving business requirements must be disabled.
• Trust relationships between systems may only be introduced according to business requirements, must be documented, and must be approved by InfoSec.
• Services and applications not for general access must be restricted by access control lists.
• Insecure services or protocols (as determined by InfoSec) must be replaced with more secure equivalents whenever such exist.
• Remote administration must be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks. Where a methodology for secure channel connections is not available, one-time passwords

(DES/SofToken) must be used for all access levels.
• All host content updates must occur over secure channels.
• Security-related events must be logged, and audit trails saved to InfoSec-approved logs. Security related events include (but are not limited to) the following:
o User login failures.
o Failure to obtain privileged access.
o Access policy violations.
o InfoSec will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

3.3. New Installations and Change Management Procedures
All new installations and changes to the configuration of existing equipment and applications must follow the following policies/procedures:
o New installations must be done via the *DMZ Equipment Deployment Process*.
o Configuration changes must follow the Corporate Change Management (CM) Procedures.
o InfoSec must be invited to perform system/application audits prior to the deployment of new services.
o InfoSec must be engaged, either directly or via CM, to approve all new deployments and configuration changes.

3.4. Equipment Outsourced to External Service Providers
The responsibility for the security of the equipment deployed by external service providers must be clarified in the contract with the service provider and security contacts, and escalation procedures documented. Contracting departments are responsible for third party compliance with this policy.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
External service providers found to have violated this policy may be subject to financial penalties, up to and including termination of contract.

Ethics Policy

1.0 Purpose
COS Care's purpose for this ethics policy is to establish a culture of openness, trust and integrity in medical practices. Effective ethics is a team effort involving the participation and support of every COS Care employee. All employees should familiarize themselves with the ethics guidelines that follow this introduction. COS Care is committed to protecting employees, partners, vendors, patients, and the hospital from illegal or damaging actions by individuals, either knowingly or unknowingly. When COS Care addresses issues proactively and uses correct judgment, it will help set us apart from competitors. COS Care will not tolerate any wrongdoing or impropriety at any time. COS Care will take the appropriate measures act quickly in correcting the issue if the ethical code is broken. Any infractions of this code of ethics will not be tolerated.

2.0 Scope
This policy applies to employees, contractors, consultants, temporaries, and other workers at COS Care, including all personnel affiliated with third parties.

3.0 Policy
3.1 Executive Commitment to Ethics
Executives at COS Care will always operate above reproach in all business practices and relationships in which they are acting as agents of COS Care.
Executives must disclose any conflict of interests regard their position within COS Care.

3.2 Employee Commitment to Ethics
COS Care employees will treat everyone fairly, have mutual respect, promote a team environment, and avoid the intent and appearance of unethical or compromising practices.
Employees will adhere to all hospital values regarding honesty and integrity.
Employees must disclose any conflict of interests regard their position within COS Care.
Employees will help COS Care to increase patient and vendor satisfaction by providing quality care and timely response to situations.

3.3 Maintaining Ethical Practices
COS Care will reinforce the importance of the integrity message and the tone will start at the top. Every employee, manager, and director needs to consistently maintain an ethical stance and support ethical behavior.
Employees at COS Care should encourage open dialogue, get honest feedback, and treat everyone fairly, with honesty and objectivity.
COS Care has established a best practice disclosure committee to make sure the ethical code is delivered to all employees and that concerns regarding the code can be addressed.

3.4 Unethical Behavior
COS Care will avoid the intent and appearance of unethical or compromising practice in relationships, actions and communications.
COS Care will not tolerate harassment or discrimination.
Unauthorized use of hospital operational, personnel, financial, source code, & technical information integral to the success of our hospital will not be tolerated.

COS Care employees will not use corporate assets or business relationships for personal use or gain.
COS Care employees will not share, post on Facebook, Twitter, Instagram, share verbally or in writing any proprietary information, schematics, designs, or concepts, that have been deemed protected by hospital policy.

4.0 Enforcement
Any infractions of this code of ethics will not be tolerated and COS Care will act quickly in correcting the issue if the ethical code is broken.
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Internet Use Policy

These guidelines are intended to help you make the best use of the Internet resources at your disposal. You should understand the following:

1. COS Care provides Internet access to staff to assist them in carrying out their duties for the hospital, not for employees to check Facebook, purchase personal items from Amazon, or watch pornographic videos.

2. You may only access the Internet by using COS Care content scanning software, firewall and router.

3. You will comply with the following guidelines:

DO

4. Do keep your use of the Internet to a minimum
5. Do check that any information you access on the Internet is accurate, complete and current (use of SNOPES is encouraged).
7. Do respect the legal protections to data and software provided by copyright and licenses (do not illegally download music or videos).
8. Do inform the I.T. Department immediately of any unusual occurrence.

DO NOT

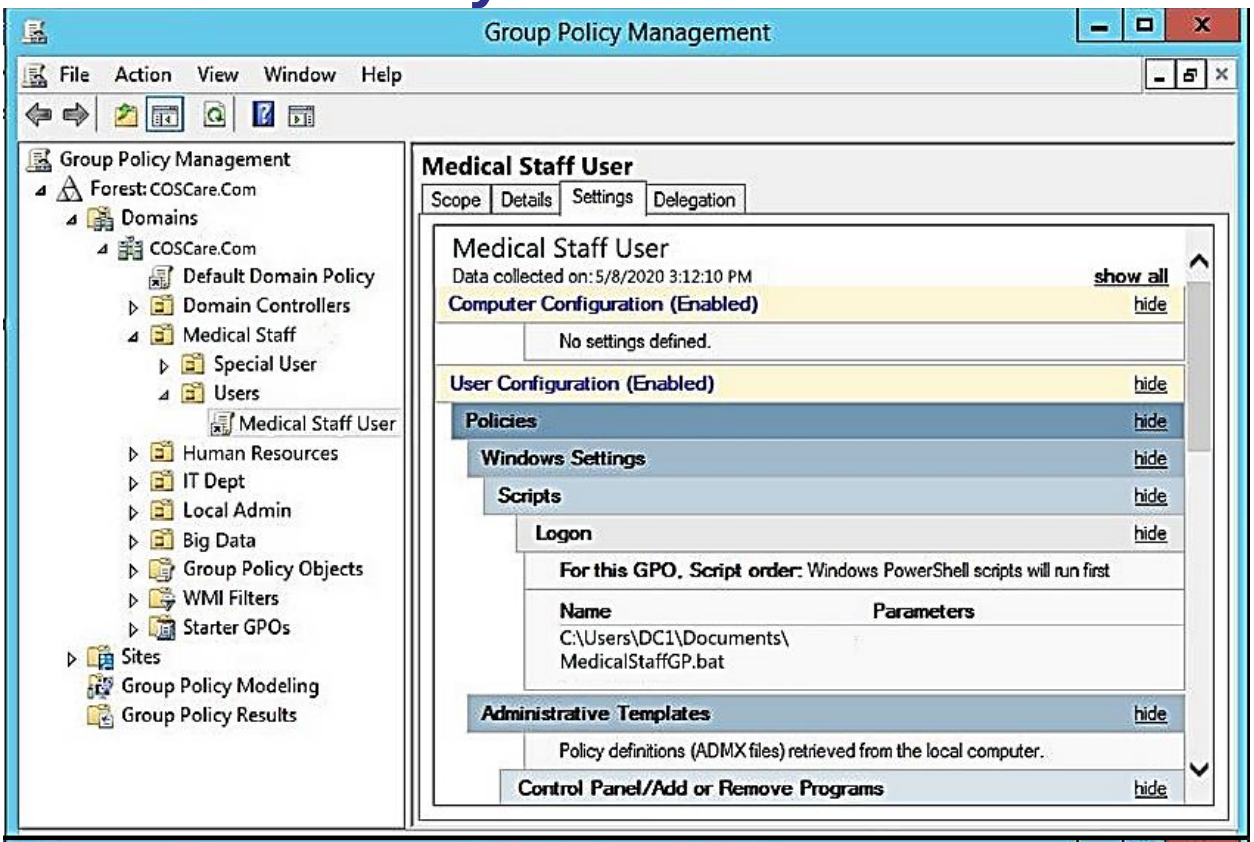
9. Do not download text or images which contain material of a pornographic, racist or extreme political nature, or which incites violence, hatred or any illegal activity.
10. Do not download applications from Internet sites.
11. Do not attempt to install downloaded software upon the COS Care's computer equipment.
12. Do not use the COS Care's computers to make unauthorized entry into any other computer or network.
13. Do not disrupt or interfere with other computers or network users, services, or equipment. Intentional disruption of the operation of computer systems and networks is a crime under the Computer Misuse Act 1990, and you will be punished under the full extent of the law.
14. Do not represent yourself as another person.

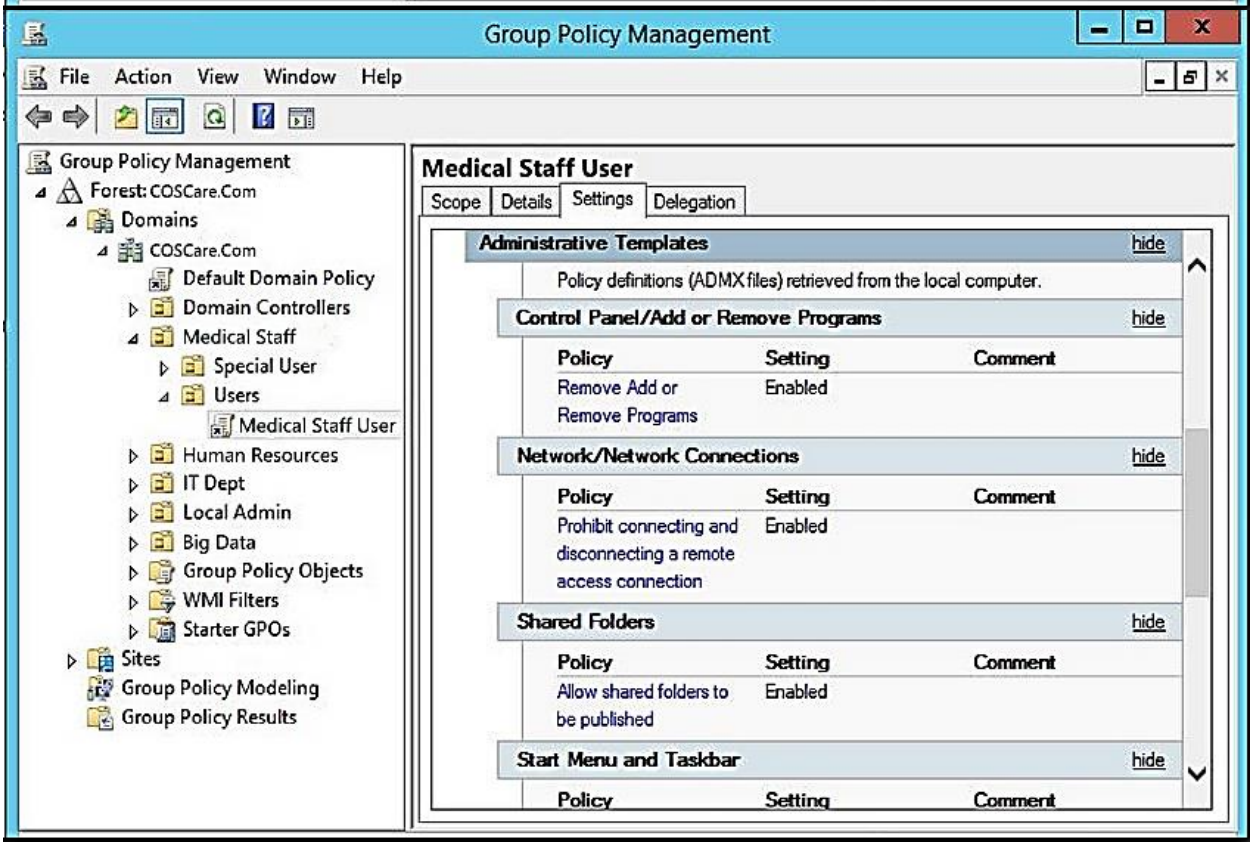
15. Do not use Internet access to transmit confidential, political, obscene, threatening, or harassing materials.

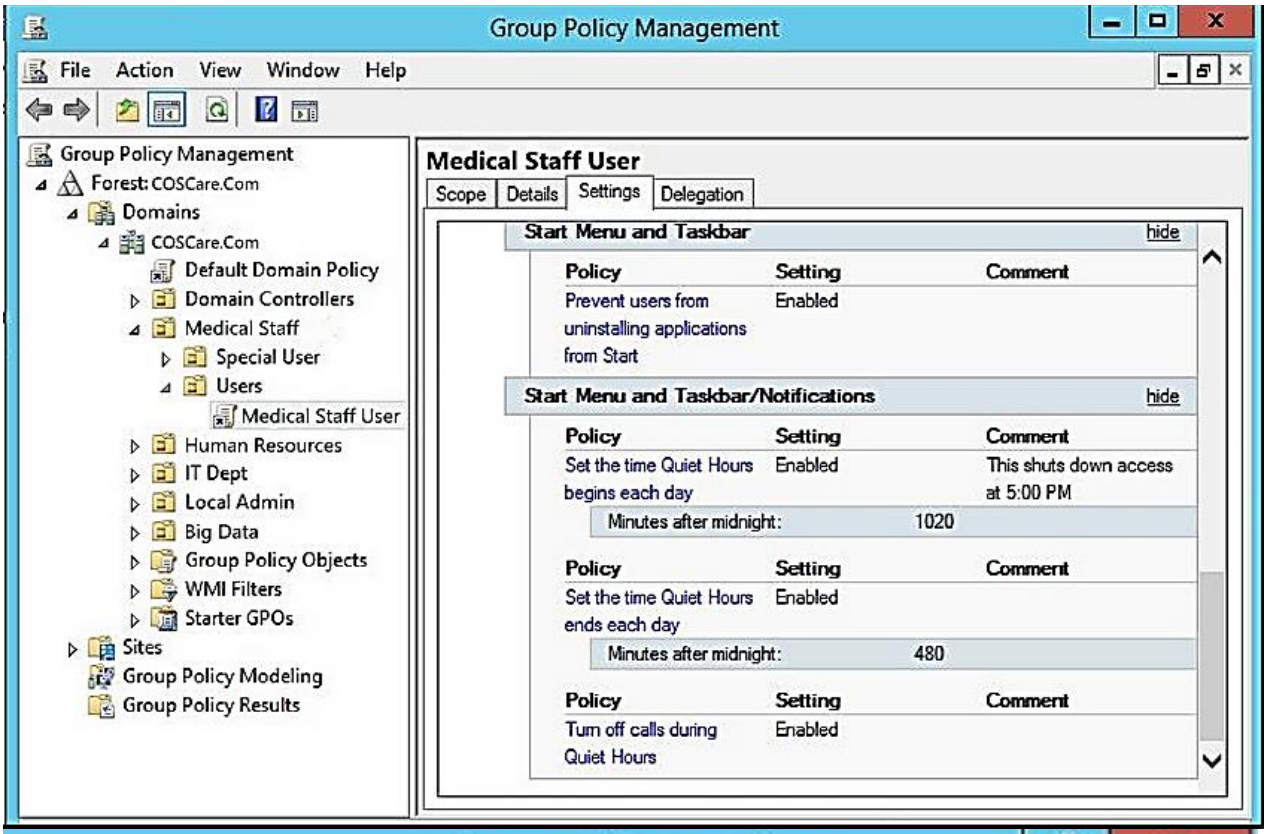
Please note the following

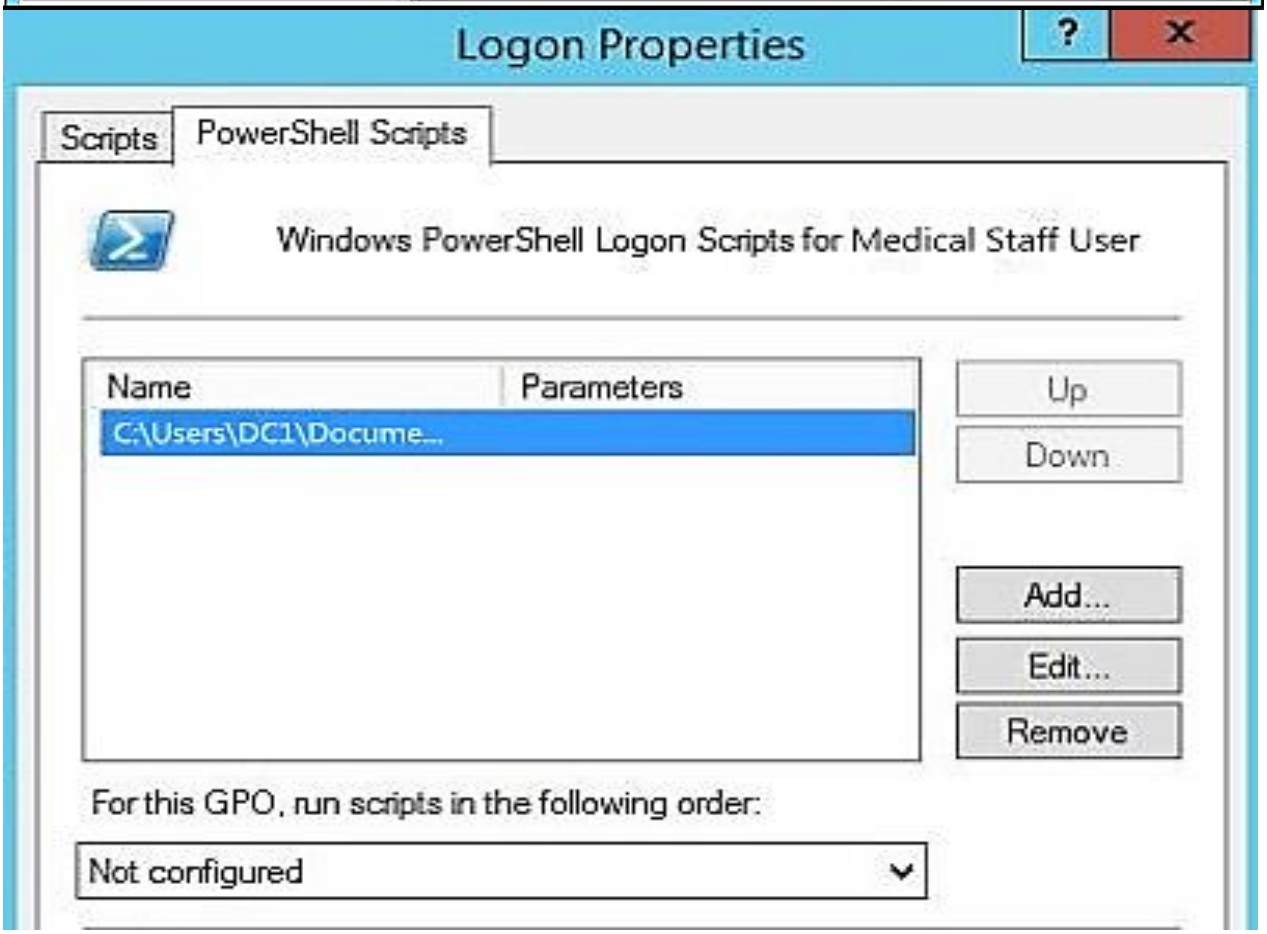
All activity on the Internet is monitored and logged (including any traffic via incognito mode).
All material viewed is scanned for viruses.
All the content viewed is scanned for offensive material.
If you are in any doubt about an issue affecting Internet Access, you should consult the IT Department.
Any breach of COS Care's Internet Acceptable Use Policy may lead to disciplinary action up to and including termination.

Technical Policy







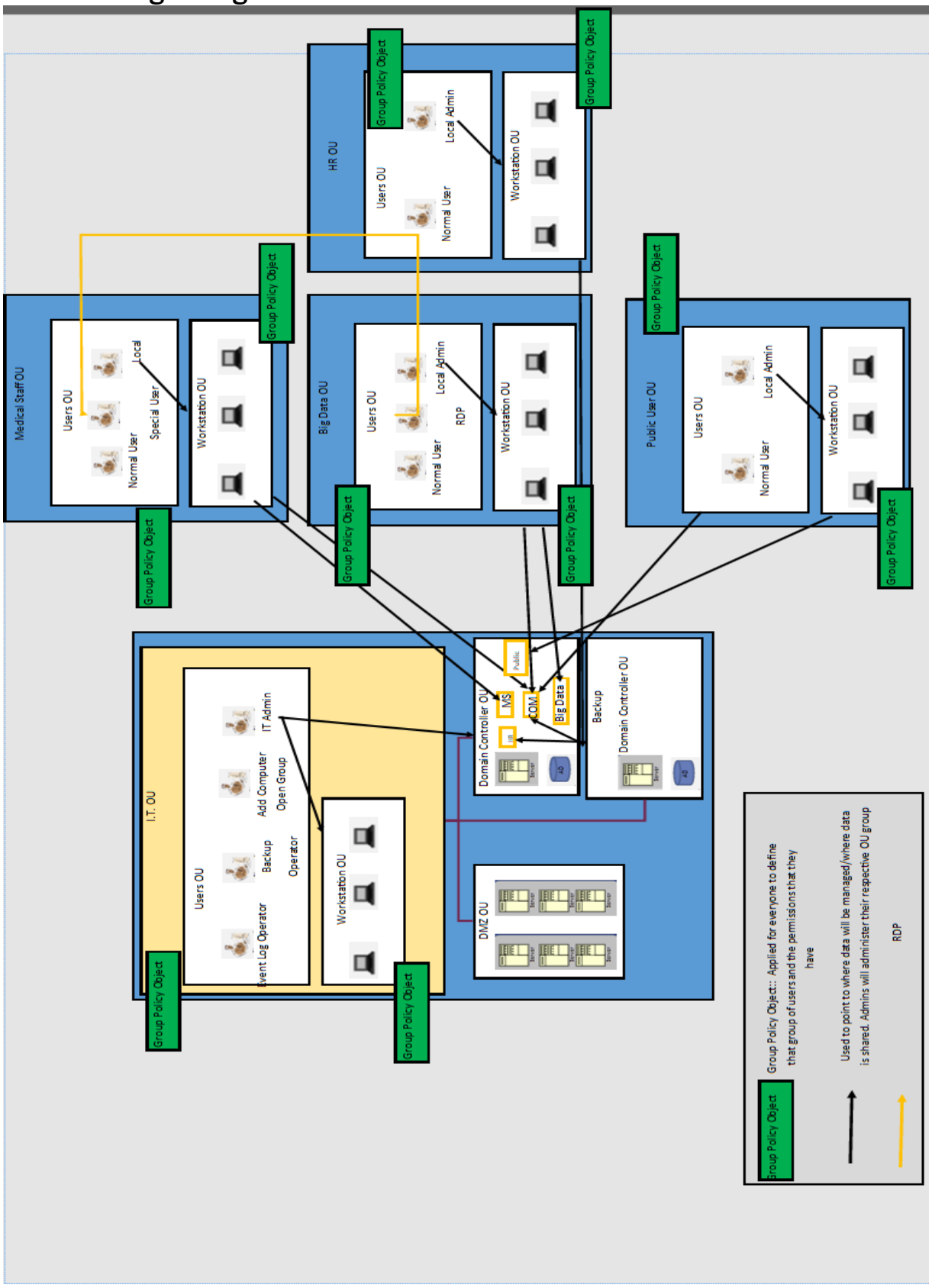


- Shown above are the limitations for the medical staff group. These restrictions change per group, medical staff is just used as an example.

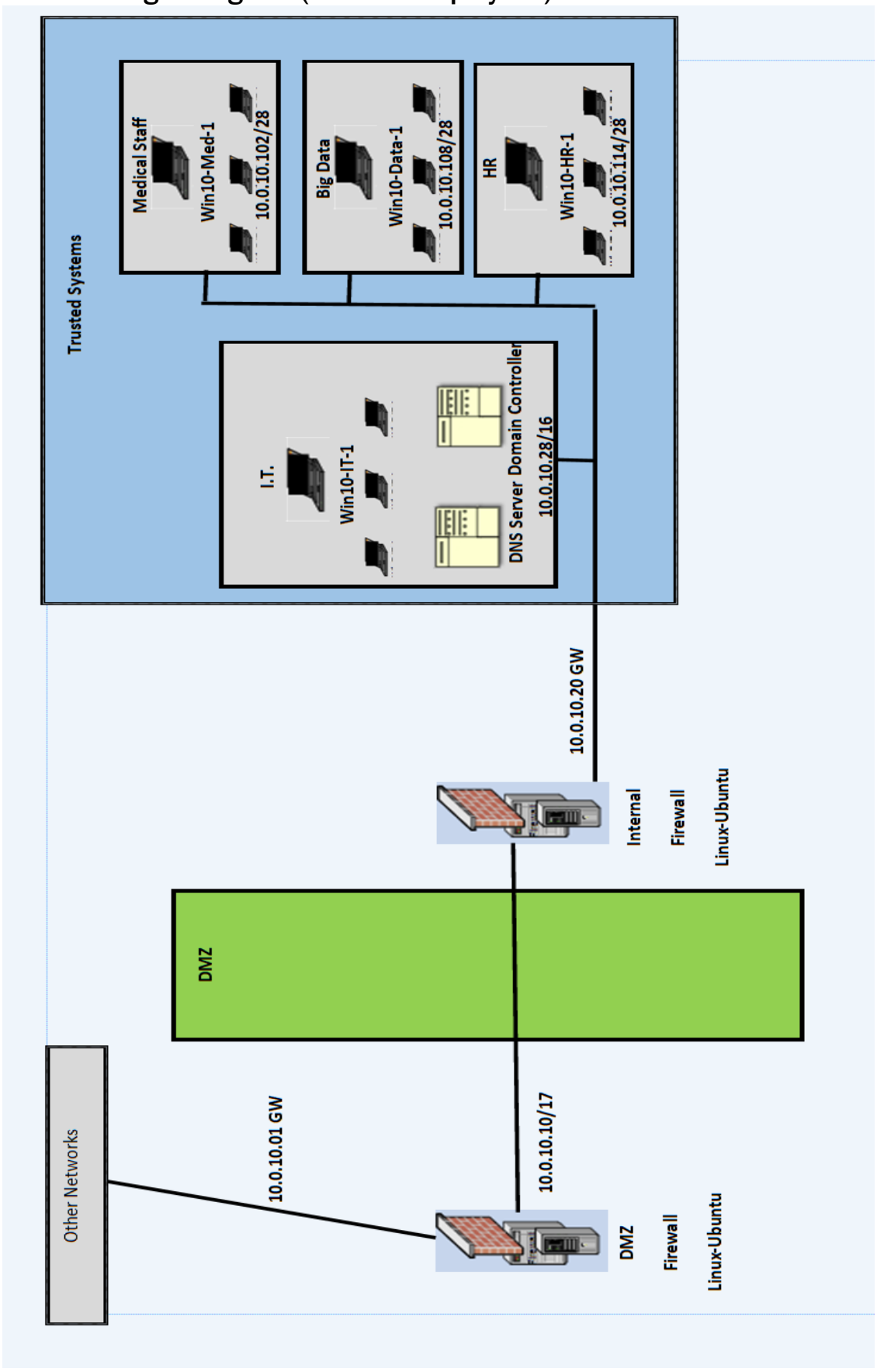
- User workstations will be locked for medical users at 5:00 PM-8:00 AM to ensure that no medical data is leaked. This can be overridden from special access from the Local Admin for Medical Staff.
- Upon login, the batch script MedicalStaffGP.bat is used to ensure permissions and file integrity is kept. Also used to ensure company image is correct.
- All medical staff will need to consult their local admin for installing or uninstalling any medical applications. Medical Staff do not have permission to perform these tasks.
- Shared files and RDP are disabled at 5:00 PM to ensure data integrity.
- These permissions can be altered per working hours or specific responsibilities of each OU.

Logic Diagrams

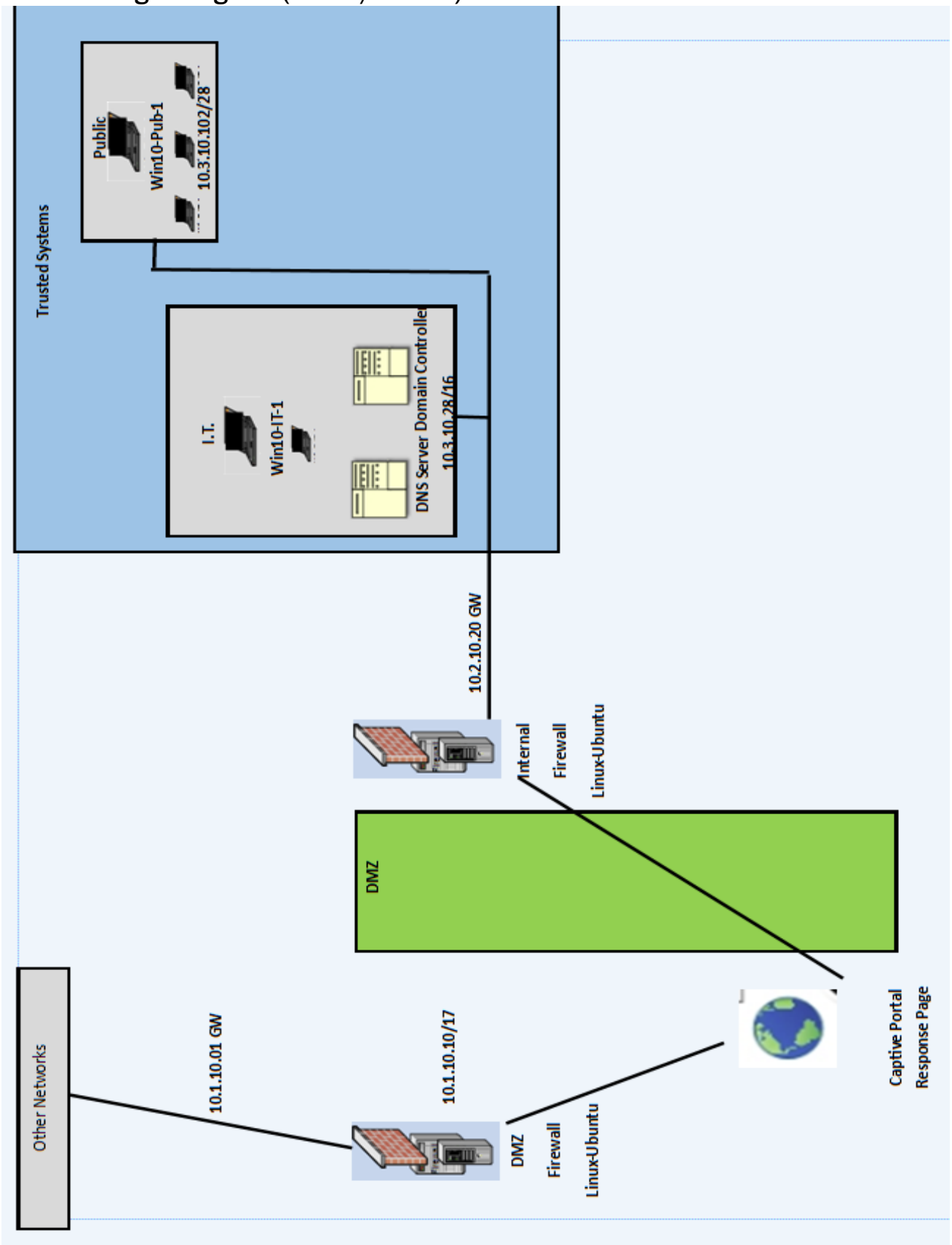
Business Logic Diagram



Network Logic Diagram (Trusted Employees)



Network Logic Diagram (Public/Guests)



Logic Diagram Explanations

Business Logic Diagram
Implementation runs from batch scripts that it contained in the technical policy above. This policy will protect data at the workstation and the department level based on their Group Policy. Each domain will contain own local system admin, for quicker response, as well as more knowledge of specific OU systems. The IT OU will contain logging operator, backup operator, an Overall IT Admin, and an operator in case a new group needs to be created. This IT OU will manage the primary and secondary DMZs/ Domain Controllers and all their components. All computers for the IT OU will run on Ubuntu, with upgrade necessary if the business expands.

All other departments (Medical Staff, Big Data, Public, and HR) will have a roughly similar infrastructure with a group policy defining each. Each will have a Local Admin controlling the workstations in their respective OU. These Local Admins will also update their group policies when necessary to allow or deny new applications, or anything that can be seen as malicious activity. All necessary data regarding statistics that is not personal health information (PHI) such as statistics local to COSCare are sent to a computer on the Medical Staff OU. This computer will have port 3889 open for the big data team to grab data, but not have access to anything else within the medical files.

Network Logic Diagram (Trusted Employees)
All inbound and outbound network activity will go through the DMZ which has a firewall contained to notices any initial abnormalities in the network. Once passed through the initial DMZ, another firewall will ensure that the correct user is entering the correct area. This firewall will also contain an intrusion detection system (IDS) to track any malicious activity. This IDS can be manipulated where budget permits, with possible growth maybe invest in an intrusion prevention system (IPS). Once these firewalls are bypassed, the network routes to the correct IP through the DNS and goes to the trusted system. With further growth, firewalls can be implemented at the department level to heighten security measures.

Network Logic Diagram (Public/Guests)
All public users can connect to the guest Wi-Fi and are brought to a DMZ that ensures the device is safe to prevent malware entering the network. All users must enter the captive portal where they will have to sign an agreement as defined in the Captive Portal Policy and then be brought to the following home page of COSCare.com. When the user signs the captive portal agreement, another firewall ensures nothing has changed and it is the same device attempting to enter the network. A Local IT Admin will ensure that there are no attacks attempted on the network, and that no attempts are made to enter the Private Network.

User Accounts

System Administrator:
The System Admin is responsible for upkeep the IT department. They maintain the systems software, along with all software updates to ensure network system security. will all of COS Care's computer hardware needs, to include server and network maintenance. The System Admin has local access to all workstations in the IT department and has remote access to the COS Care's main and backup domain controller's. This person must also create groups for the COS Care, to include local administrator accounts for each group created.

Local Administrators:
The Local Administrator is created by the System Administrator. Each group has its own Local Administrator. These users do not have access to the administrator account on the network but are given more privileges than the other users. The Local Admin responsibilities include adding each of the local users, installing the department applications, updating the system, and installing any patches for their department.

Backup User:
This user only has local access to the IT department. This person performs a backup of the server every Friday to a secure external server in an offsite facility.

Log Monitoring User:
This user monitors all system logs for the company. This user only has local access to the IT department.

Medical Staff:
The Medical Staff are the general population of employees within COS Care. This group of users have very restricted access to both the network and their individual workstations. At no time will the Med Staff be allowed to install or uninstall any applications on any workstation they have access to. These user's activity will be monitored by the Local Administrator, the log monitoring user, and the System Admin.

Special Users:
The special users will be similar to the Medical Staff however, they will have remote access to the other department's workstations (excluding the IT department). COS Care's special user groups would include BigData user's, Medstaff, Human Resources and public.
• BigData users will have limited access to the medical staff to analyze data. HAS RDP ACCESS to a reserved access to medical to port 3389.
•Med staff will have permissions on reading and writing their own files, however all applications will need to be approved by the Local IT Admin before installing on their workstation.
• The public will have the least amount of access when it comes to the network (Basic WiFi comes to mind).
• Human Resources has standard use for all personal data.

Future Growth

Some of the main components we must consider for the growth of COS Care is our systems reliability, scalability, cost, and its manageability. We want all our systems to be able to handle the basics of computing and productivity. Most machines will be running all day long with an occasional reboot for updates and patches. The system needs to be able to adapt to the needs of COS Care. This will allow COS Care to provide services needed from the public. With the growth of the hospital comes the manageability of its system. This is laid out in the user's section of the proposal, where COS care plans on limiting the access of each user to only be able to use the necessary programs of that user. Along with the full operation of COS Care we will have to back up our data. At first, we will have an internal server with our data. However, if anything happened, we need to have an offsite backup just in case of emergency.

With the expansion of COS Care, we will need an infrastructure that will sustain it. Linking with Azure/AWS to have a virtual system, will allow COS Care easy access to expand each new department with ease. The virtual systems will also minimize the requirements of the physical systems which could help with limiting cost for the hospital. Since the systems would not need physical space to store data it would all be on the cloud. This would also give COS Care a second way to access its data. Another item that each new department would bring is the need for additional firewalls, switches, servers, and computers.

Further development in COS Care will also bring in the need for additional users. With each new user group, we will implement RBAC (Role Based Access Control). By doing this it will restrict each groups access to authorized systems. While allowing each group the ability to become more define. Possible changes could implement more user groups, such as, doctors, nurses, and pharmacy to name a few. One last thing COS Care would do is to add each new group/department to the website. While expanding the IT group will need to keep the system updated and the security/policies within the network/domain.

Linux Documentation

Add a New user script

This makeuser script makes the process of adding a new employee to a group, while also ensuring that the individual has the correct permissions. The second image is an example of how the user is added. This script is key for company growth to ensure that all users are logged when performing any action.

```
#!/bin/bash

if [$(id -u) -eq 0];then
        read -p "Enter Username:"username
        read -s -p "Enter Password:"password
        egrep "^$username" /etc/passwd >/dev/null
        if[ $? -eq 0 ];then
                echo "$username exists!"
                exit 1
        else
                pass=$(perl -e 'print crypt($ARGV[0], "password")' $password)
                useradd -m -p "$pass" "$username"
                [ $? -eq 0] && echo "user has been added ot the system" || echo  "failed to add"
        fi
else
        echo"only IT may add users"
        exit 2
fi
```

```
/etc$ sudo bash makeuser.sh
Enter username : drBob
Enter password : User has been added to system!
```

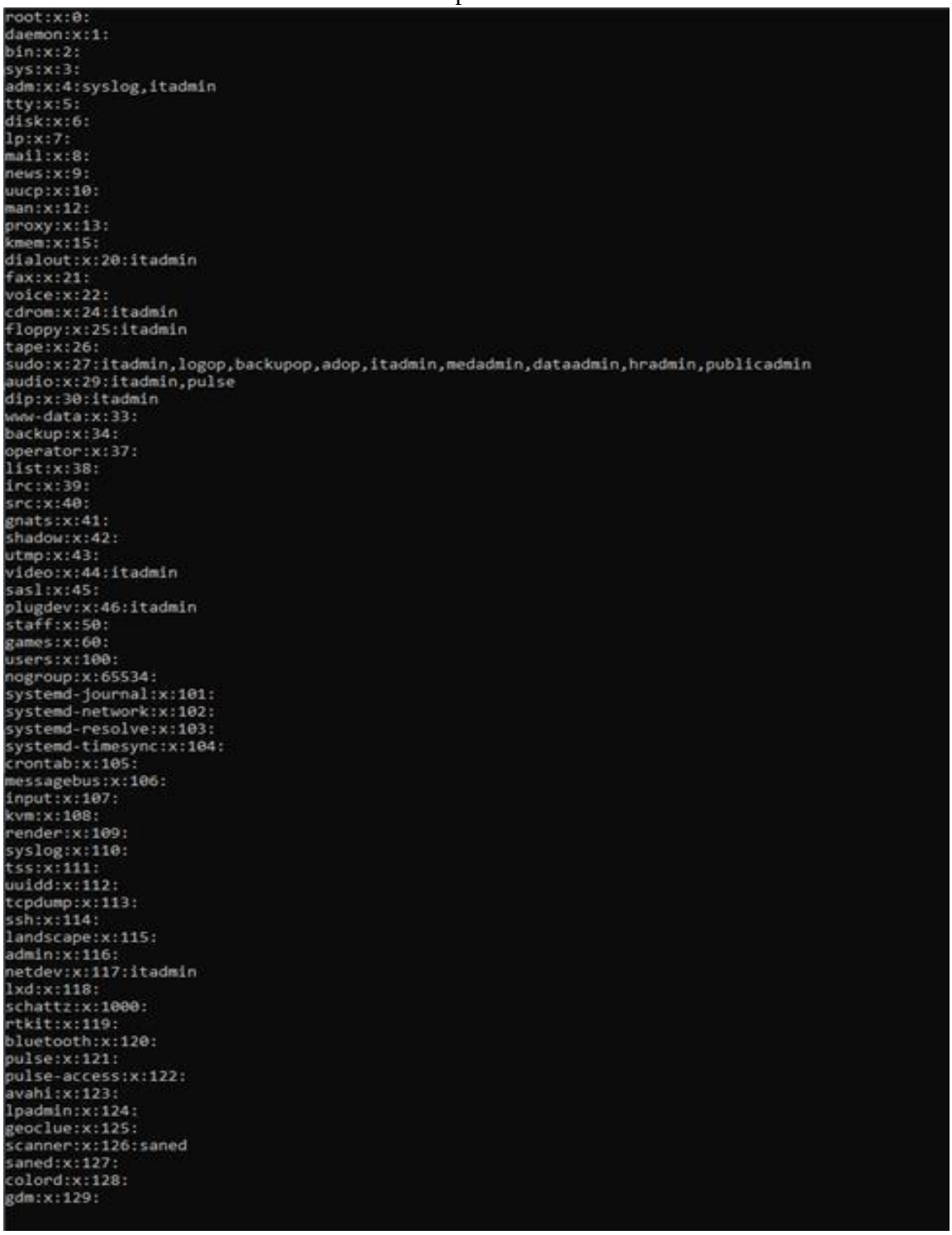
Sudoers File

This file lists everyone's respective groups, and their permissions involved. There are warnings for when the user logs in, where everything is kept, who has Sudo rights, password timeouts. Currently, only members of the IT group can run Sudo commands due to this file being meshed with the /etc/group file.

```
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"
Defaults        log_file ="/var/log/sudo.log"
Defaults        lecture="always"
Defaults        badpass_message="password is wrong please try again"
Defaults        passwd_trys=3
Defaults        passwd_timeout=30
Defaults        log_input,log_output
# Host alias specification

# User alias specification
User_Alias IT = logop, backupop,addop,itadmin,medadmin,dataadmin,hradmin,publicadmin
User_Alias MED= nurse1, nurse2, dr
User_Alias HR = HR1, HR2
User_Alias BIG_DATA = bd1
# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%root ALL=(ALL) ALL
%IT   All=(All) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
```

Group File

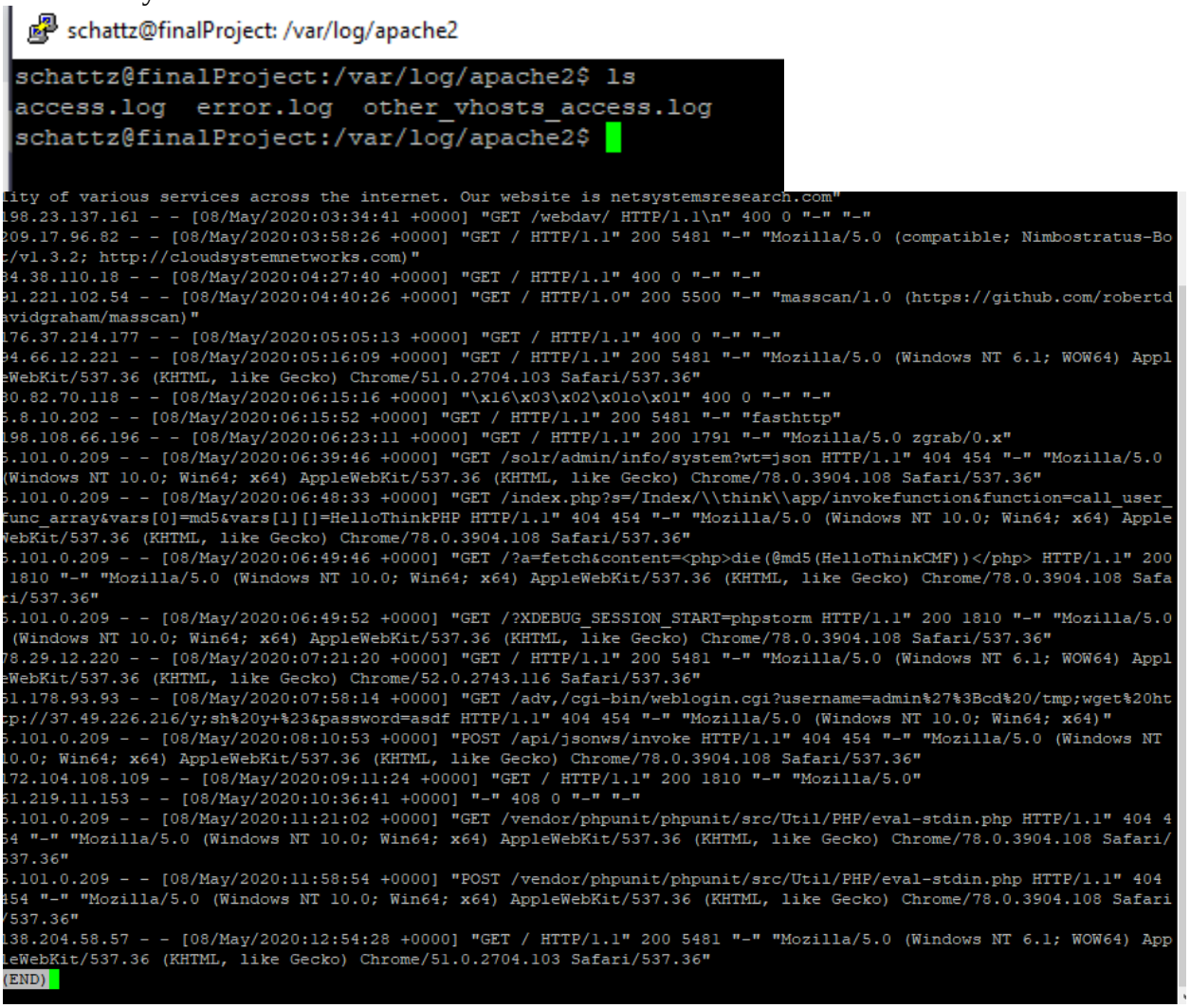
The group file defines the groups to which users belong to. All the administrators currently have access to change anything about their respective department, however everything is logged just in case something does go wrong. This permissions can be further limited with consensus of the IT Department.



```
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,itadmin
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:itadmin
fax:x:21:
voice:x:22:
cdrom:x:24:itadmin
floppy:x:25:itadmin
tape:x:26:
sudo:x:27:itadmin,logop,backupop,adop,itadmin,medadmin,dataadmin,hradmin,publicadmin
audio:x:29:itadmin,pulse
dip:x:30:itadmin
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:itadmin
sasl:x:45:
plugdev:x:46:itadmin
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
systemd-journal:x:101:
systemd-network:x:102:
systemd-resolve:x:103:
systemd-timesync:x:104:
crontab:x:105:
messagebus:x:106:
input:x:107:
kvm:x:108:
render:x:109:
syslog:x:110:
tss:x:111:
uuidd:x:112:
tcpdump:x:113:
ssh:x:114:
landscape:x:115:
admin:x:116:
netdev:x:117:itadmin
lxd:x:118:
schattz:x:1000:
rtkit:x:119:
bluetooth:x:120:
pulse:x:121:
pulse-access:x:122:
avahi:x:123:
lpadmin:x:124:
geoclue:x:125:
scanner:x:126:saned
saned:x:127:
colord:x:128:
gdm:x:129:
```

Apache Logs

Below are the Apache logs to ensure that the website infratructure was done correctly. All information of the website is stored in the access.log, which is monitored in coordinance with the Audit Policy.



Website Screenshots

Below are two sample screen shots of the front facing website. These are located on the company network and were made with Apache. These websites can only be viewed by being on the company website. Each link can be accessed, local it admins can limit the further data provided by these sites by ensuring respective permissions.

IP-Tables

Shows all configured routes, can also be altered in Azure to ensure proper security and more of a GUI.

```
#!/bin/bash
# Removes all configured rules
iptables -F

# Defaults
iptables -p INPUT DROP
iptables -p FORWARD DROP
iptables -p OUTPUT DROP

# DC1 to DNS
iptables -A FORWARD -s 10.0.10.21 -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -s 10.0.10.29 -p udp --dport 53 -j ACCEPT

#Data and Med Comms
iptables -A OUTPUT -s Data ip -d Med ip -j ACCEPT
iptables -A INPUT -s Med ip -d Data ip -j Accept

# Allow Outbound
iptables -A FORWARD -s 10.0.11.20/27 -d 0/0 -j ACCEPT

# Allow already made connects
iptables -A FORWARD -s 0/0 -m state --state ESTABLISHED -j ACCEPT

# Allow LocalHost
iptables -I INPUT -i lo -j ACCEPT
iptables -I OUTPUT -o lo -j ACCEPT

# ALLOW SSH
iptables -I INPUT -i ens192 -p tcp -s 10.0.11.1/24 --dport 80 -j ACCEPT
iptables -I INPUT -i ens192 -p tcp -s 10.0.11.1/24 --dport 443 -j ACCEPT
iptables -I INPUT -i ens192 -p tcp -s 10.0.11.1/24 --dport 53 -j ACCEPT

iptables -I INPUT -p tcp -s 10.0.11.1/24 --dport 80 -m state --state ESTABLISHED -j ACCEPT
iptables -I INPUT -p tcp -s 10.0.11.1/24 --dport 443 -m state --state ESTABLISHED -j ACCEPT

# ICMP
iptables -I OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
iptables -I INPUT -p icmp --icmp-type echo-reply -j ACCEPT
```