Palmetto Co-Op Doctors Clinic
Compassionate and Quality Health Care
https://pcdc-sc.com

Introduction

April 8, 2024

Palmetto's Co-Op Doctors Clinic (PCDC) is the Lowcountry's premier choice for compassionate and quality health care. PCDC has doctors available in every specialty and is always accepting new patients! Our doctors and nurses are caring, attentive and always put patient safety and satisfaction first. PCDC's state-of-the-art equipment and skilled team ensure that patents can find services such as laboratory work, x-rays, and other scans all in one location, rather than having to go to another facility. With such a large team and an array of specialties, patients are always able to come to PCDC to receive treatment for a range of illnesses and injuries. Our customer service, friendly staff and attention to detail are what keeps our patients healthy and satisfied.

PCDC strives to continue offering urgent and primary care services with flexible hours to keep customers happy and coming back. We pride ourselves on providing timely and convenient health care services. We hope to see you next time you need health care of any kind!

PALMETTO
CO-OP
DOCTORS
CLINIC

Compassionate and Quality Health Care

Palmetto Co-Op Doctors Clinic
Compassionate and Quality Health Care
https://pcdc-sc.com

April 8, 2024

Blue Team,

Welcome to the Palmetto Co-Op Doctors Clinic (PCDC) team, where you will oversee the information technology department that maintains all the clinic's online functions. Your team will be responsible for ensuring all the clinic's critical services are operational and patients remain satisfied.

As new employees of PCDC's support team, each of you will complete various roles of system administrator duties ensuring continuous service to our clients 24/7. This includes maintaining and protecting financial and patient databases, internal communication systems, API interfaces, and many other critical system functions. The databases will possibly contain Personal Identifiable Information (PII) and patient's Protected Health Information (PHI) that must be protected at all times.

Your team must ensure Confidentiality, Integrity, and Availability is maintained using secured, encrypted data transmission protocols, firewalls, VPN tunneling for remote desktop support, and professional communication to multiple clients as needed on a day-to-day basis. Your team must also answer trouble calls and special requests from clinic directors, doctors, and patient representatives.

As the risk of data breaches, ransomware, phishing, and denial of service attacks continue to grow, it is paramount the security of our infrastructure be of the utmost importance to preserve our patient's satisfaction. PCDC has hired your team to ensure PCDC's databases are secured, company and patient information is protected, and professional service is always provided. Unfortunately, the previous team abruptly vacated their positions, so we cannot guarantee the current state of any service or of the network diagram.

PCDC is confident your team will help our airline not only maintain but improve our excellent customer service record and reputation among patients. We are excited to have you as part of our exceptional team!

Welcome to Palmetto Co-Op Doctors Clinic (PCDC)!

Regards,

Dr. Hannibal Lecter
CMO

TABLE OF CONTENTS

1.0 ACCOUNT INFORMATION 1
1.1 Initial Password List 1
1.2 Password Changes 1
1.3 Email Access 1
2.0 NETWORK OVERVIEW 1
2.1 Backups and Recovery 1
2.2 Active Defense 2
2.3 Incident Reporting 2
2.4 Firewall Requests 2
2.5 Laptop Information 2
2.6 Out of Band Information 3
2.7 Out of Band Email 3
2.8 Enabling Multi-Factor Authentication 4
2.9 Gold Team Help Desk 7
3.0 TEAM ASSESSMENT 7
3.1 Scoring 7
3.2 Injects 8
4.0 ADDITIONAL INFORMATION 8
4.1 Blue Team Tools and Supplies 8
4.2 Scripting 8

LIST OF APPENDICES

Appendix A 1
Appendix B 2
Appendix C 3

1.0 ACCOUNT INFORMATION

1.1 Initial Password List

At the start of the day, your team will be provided with your initial username and password information for all assigned assets.

1.2 Password Changes

Changes of domain user accounts need to be reported to the Gold Team. Please submit password changes to the Gold Team Ticketing service to lessen service check downtime. Failure to promptly report changes to domain user accounts can negatively impact service checks from the competition scoring engine.

1.3 Email Access

Blue Teams will access their web-based email through the following web address: **https://mail.blueXX.pcdc.local** which is in scope. Any email from @pcdc.local is out of scope from the Red Team, however, that does not mean all emails from @pcdc.local are credible. All emails should be evaluated properly, and any suspicious activity should be reported immediately. Hannibal Lector (hannibal.lector@blueXX.pcdc.local) is the Chief Medical Officer for Palmetto Co-Op Doctors Clinic and will be receiving various messages throughout the day. You are required to monitor this account at all times.

2.0 NETWORK OVERVIEW

Your assigned network consists of virtual machines that are accessed via standard remote access protocols (RDP and SSH) from the assigned laptops. Usernames and passwords for all assets will be provided in the Initial Password List at the start of competition. An old network diagram was found and is located in Appendix A. Your network will consist of a mix of Windows and Linux operating systems.

2.1 Backups and Recovery

Teams do not have access to create backups of VMs, nor to recover a VM. Recovery requests can be submitted via a ticket to the Gold Team Help Desk. Select ***Request*** as the ticket category and use the following format:

SUBJECT: Recovery Request
BODY:
Team #: ___________
Request: ___________
Justification: ___________

Please note that recovery comes with a **substantial cost** and reverts the machine to its initial operating condition.

2.2 Active Defense

While this term is still being defined in industry (some say it includes offensive capabilities and others say it does not), we are referring to Defending Forward – countering of preventing a perceived cyber-attack by taking the fight to your adversary with the goal of taking away their ability to perform offensive cyber operations against you. This is **not permitted under any circumstances**. Teams should keep their actions within their own assigned assets, unless explicitly permitted by Dr. Bruce Banner, Chief Information Systems Officer (CISO).

2.3 Incident Reporting

Accurate incident reports that can be verified will net your team a modest number of points in the end-of-day team assessment. Incident reports must contain a description of how and what occurred (including source and destination IP addresses, timelines of activity, passwords cracked, access obtained, damage done, etc), a discussion of what was affected, and a remediation plan. Overly inaccurate Incident Reports, especially abuse of Incident Reports, will net no points and may result in a loss of points.

Written reports must be coherent and professional. Should you recognize that an incident has occurred, you may escalate an incident response report by submitting a ticket to the Gold Team Help Desk. Select ***Incident*** as the ticket category and use the following format:

SUBJECT: Incident Reporting
BODY:
Team #: ___________
Time(s) of Incident: ___________
Asset(s) Affected: ___________
Source (IP Address) of Attack: ___________
Description of Attack/Incident: ___________
Remediation/Plan to Resolve: ___________

2.4 Firewall Requests

The perimeter firewall will be managed by the PCDC, Inc Gold Team. All requests to modify the perimeter firewall must be submitted to the Gold Team via the Help Desk Ticketing system and by selecting the ticket category ***Request***. Host based firewalls may be managed by the Blue Teams.

2.5 Laptop Information

Certain programs and applications have been setup on the laptop for use during the competition. They include but are not limited to:

- puTTY (SSH)
- Remmina (RDP)
- Chrome
- KeePass

2.6 Out of Band Information

The below items are out of band. Please pay careful attention to this section.

- The laptops are out of band and are fully out of scope from the Red Team.
- The account "goldteam" on all physical machines, virtual machines and network devices is out of band and off limits for both Blue Teams and Red Team.
- All traffic and devices on the 192.168.40.0/24 network are out of band for the Red Team. Blue Teams are **not authorized** to block traffic from this network.
- Edge routers are off limits and out of band for both Blue Teams and Red Team.
- Blue Teams are **not authorized** to block traffic from 192.168.20.10.

2.7 Out of Band Email

Blue teams will be given a Stemrocks account that will be used for email, chat and Gold Team Help Desk access. This account is out of scope for the Red Team. This account will be used for inject distribution, submitting injects and access to the Gold Team Help Desk. The Stemrocks site can be reached at:

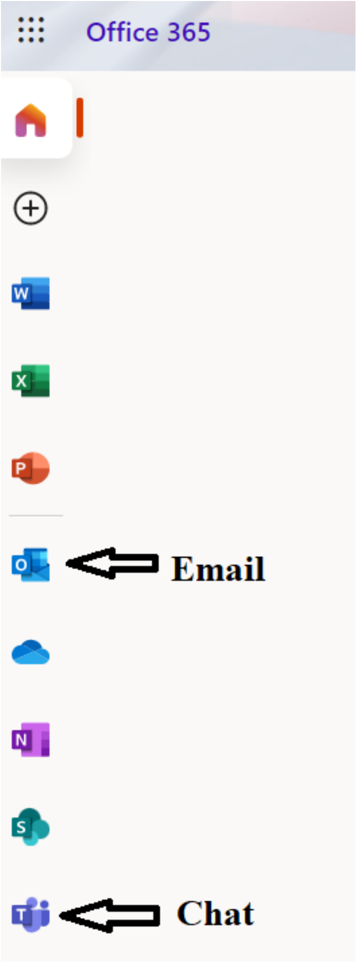
https://portal.office.com

Account format is:

HS-blueXX@stemrocks.org
COL-blueXX@stemrocks.org
PRO-blueXX@stemrocks.org

Passwords will be provided the day of competition.

Once logged in, select the Outlook application icon from the left side of the site for access to email. Select the Teams application icon for access to chat. Each Blue Team will have a pre-configured "Team/Channel" for intra-team communication only. Communication with other teams or any person(s) not a part of the respective Blue Team is **strictly prohibited.** Icons may not appear in the same order as displayed in this image.

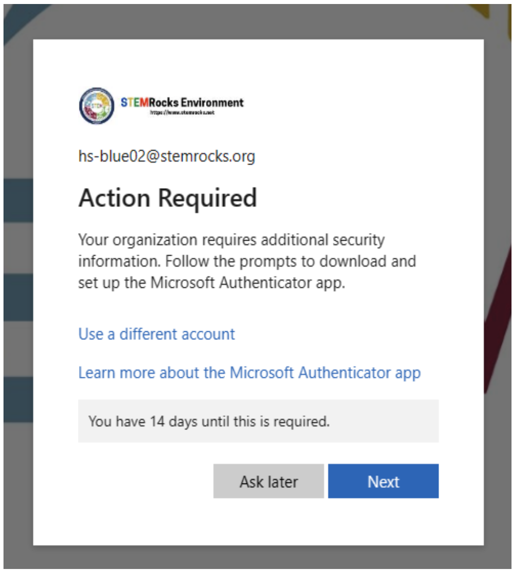


2.8 Enabling Multi-Factor Authentication

Due to Microsoft updates, the Stemrocks accounts utilized during the competition require Multi-Factor Authentication (MFA). Mobile phones are not allowed in the team area, so competitors will be required to use a personal email that is accessible via a browser. Use of the personal email for anything other than MFA is strictly prohibited, and any team caught using information stored in a personal email will come with a significant points penalty.

Follow the steps below to enable MFA:

1) Change your password (if prompted)
2) Once the password is changed, there will be a screen that says “Action Required.”



hs-blue02@stemrocks.org

Action Required

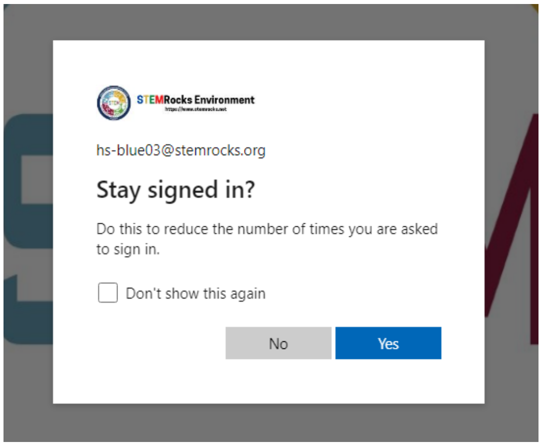
Your organization requires additional security information. Follow the prompts to download and set up the Microsoft Authenticator app.

Use a different account

Learn more about the Microsoft Authenticator app

You have 14 days until this is required.

3) Click the "Ask Later" button.
4) On the "Stay signed in?" screen, select either "Yes" or "No".



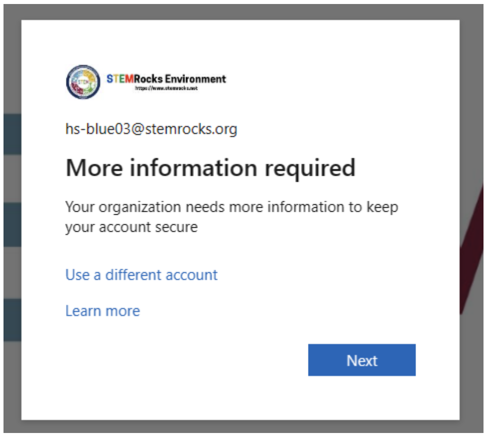
hs-blue03@stemrocks.org

Stay signed in?

Do this to reduce the number of times you are asked to sign in.

□ Don't show this again

5) Click "Next" on the "More information required" page. This may not pop up – if it doesn't, proceed to the next step.



hs-blue03@stemrocks.org

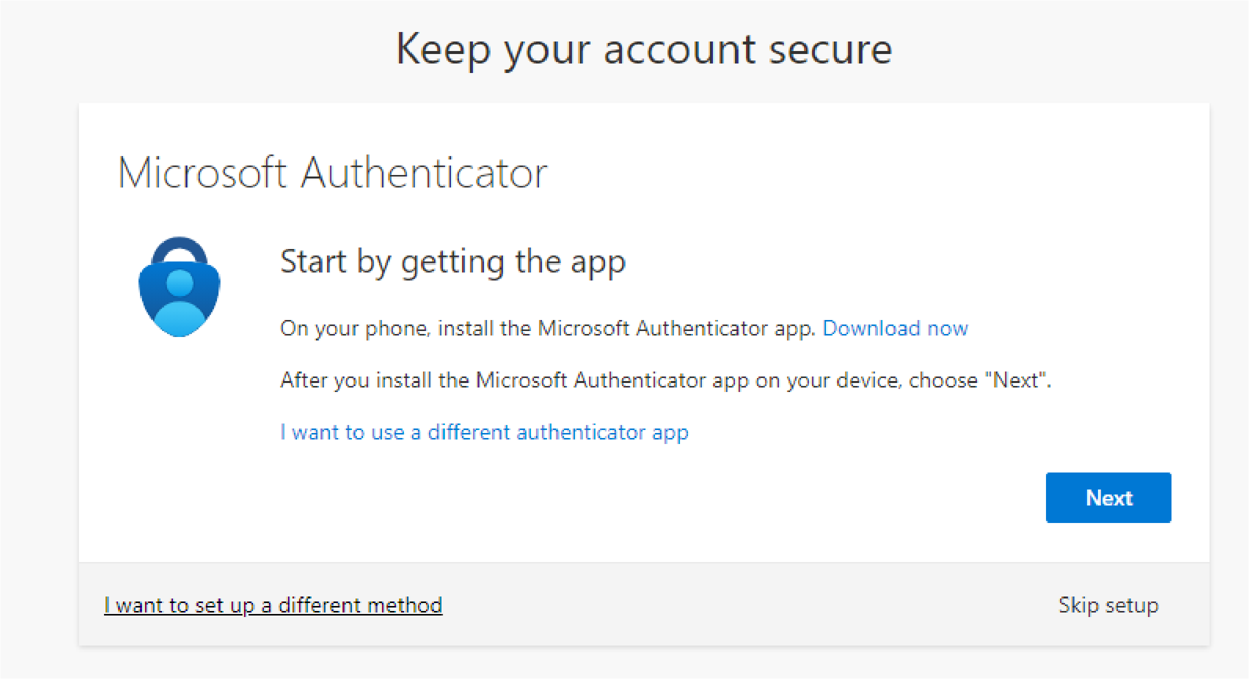
More information required

Your organization needs more information to keep your account secure

Use a different account

Learn more

6) On the “Keep you account secure” page, click “I want to set up a different method” and then select “Email” from the drop-down menu.



Keep your account secure

Microsoft Authenticator

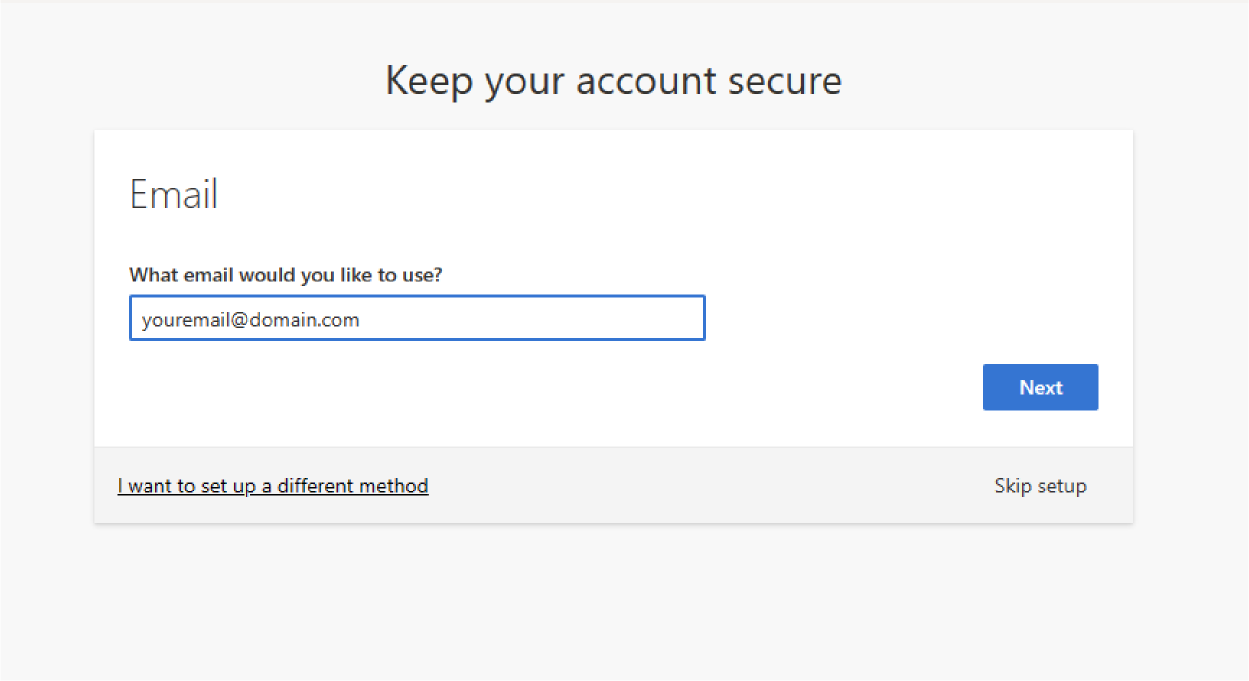
Start by getting the app

On your phone, install the Microsoft Authenticator app. Download now

After you install the Microsoft Authenticator app on your device, choose "Next".

I want to use a different authenticator app
Next
I want to set up a different method
Skip setup

7) Enter a personal email address, then click “Next.”



Keep your account secure

Email

What email would you like to use?

youremail@domain.com

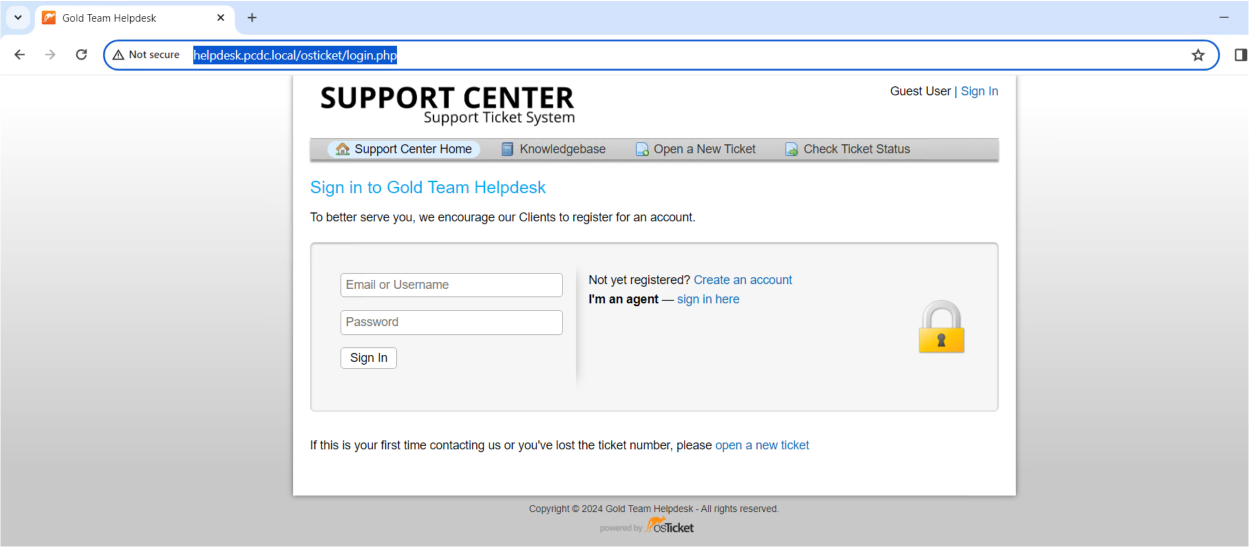
If you have any questions, let a White Team member know.

2.9 Gold Team Help Desk

There will be an online Help Desk system provided for teams to request assistance from the Gold Team. The Help Desk can be reached at:

http://helpdesk.pcdc.local/osticket/login.php.

The Gold Team Help Desk will respond as soon as possible to your ticket. The Help Desk chat function will also be available to use as needed.



Sign in to Gold Team Helpdesk

To better serve you, we encourage our Clients to register for an account.

Not yet registered? Create an account

I'm an agent — sign in here

If this is your first time contacting us or you've lost the ticket number, please open a new ticket

Copyright © 2024 Gold Team Helpdesk - All rights reserved.

powered by osTicket

3.0 TEAM ASSESSMENT

Employee performance is assessed at the end of each day. A single score is given to each team of employees.

3.1 Scoring

Scoring is based on keeping required services up, controlling/preventing unauthorized access, completing business tasks (a.k.a. injects) from colleagues, supervisors, and other departments throughout the day, and continuing to provide critical business products/services. Teams accumulate points by successfully completing these injects and maintaining services. Teams lose points by violating service level agreements, usage of recovery services, and successful penetrations by hackers, a.k.a. the Red Team.

Any team action that interrupts the scoring system is exclusively the responsibility of that team and will result in a lower score. Any team member that modifies a competition system or system component, with or without intent, in order to mislead the scoring engine into assessing a system or service as operational, when in fact it is not, may be suspended or fired. **Validation of this act will come with a significant points penalty** as it gives the Blue Team an unfair points advantage for a service that is not actually up.

3.2 Injects

If a business task (a.k.a. inject) requires multiple files for fulfillment, please compress the files into a single file in .zip format. This ensures that each inject has only one upload. Please name inject emails/files in the following format:

<teamNumber>_<injectNumber>_<injectTitle>

Injects and services are weighted evenly; it is disadvantageous to ignore injects.

There will be **NO** partial credit for late injects, so make a point to fulfill injects on-time. Inject responses that are turned in on-time will be allowed at least partial credit. Gold Team and PCDC Leadership/Judges reserve the right to change this policy as needed, and will notify all teams at the same time of any changes.

If an inject is directed to be submitted to the Gold Team Help Desk, select the ticket category ***Inject*** when creating the ticket.

4.0 ADDITIONAL INFORMATION

4.1 Blue Team Tools and Supplies

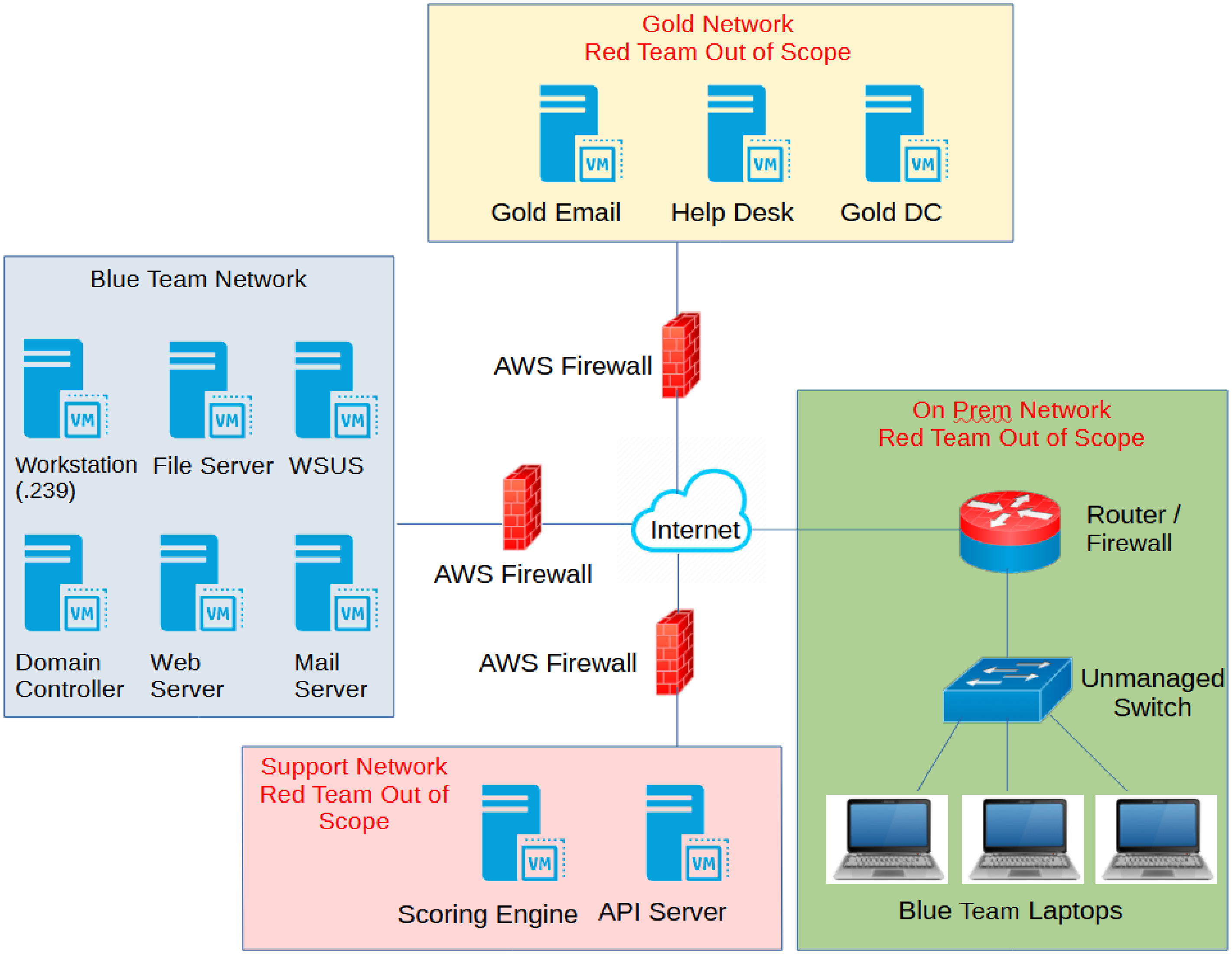
At the start of competition there will be supplies provided that could include notepads, pens, mouse pads, dry erase board markers and erases, and network cable tools. Please be sure to leave these on the team tables at the end of the day.

4.2 Scripting

Scripting during the competition is allowed, and teams are encouraged to write their own scripts. All team written scripts should be submitted to the Gold Team Help Desk for review and approval prior to use. Any resources or tools pulled down from the internet to assist with scripting shall be **publicly available and free of cost.** The use of scripts or tools not created by the team should be submitted to Gold Team by opening a Help Desk ticket, **including the citation** for the tool or resource used if applicable. Failure to notify Gold Team of script or tool usage that was not provided by the Gold Team, or the use of non-public resources **may incur a penalty.**

If the blue team has written a script in advance of the competition, it may only be brought into the competition typed and printed on a sheet of paper or hand-written in a notebook. It must be submitted to the Gold Team Help Desk including any sources used for approval.

Appendix A Network Diagram



Appendix B PASSWORD TRACKER

Username	Password	Account Description

Appendix C ORGANIZATION CHART

This list only contains the Palmetto Co-Op Doctors Clinic department leads and does not include all Palmetto Co-Op Doctors Clinic employees.

First Name	Last Name	Position	Domain Admin
Hannibal	Lector	CEO / CMO	No
Bruce	Banner	CISO	No
Mary	Ventotla	CFO	No
Walter	White	Lead Pharmacy Director	No
Joyce	Coleman	Help Desk Lead	No
Nancy	LePage	Public Relations Lead	No
Raymond	Brown	Ambulatory Services Lead	No
Dorothy	Ferro	Nursing Services Lead	No
Dylan	Darnell	Clinical Services Lead	No
Dwight	Shrute	Sales Lead	No
Jonathan	Vader	Executive Assistant	No
Juan	Griffin	Lead Enterprise Administrator	Yes
Jennifer	Bailey	Lead Network Administrator	Yes
Kathryn	Soulis	Lead Web Developer	No

This Page Intentionally Left Blank