WCU Campus Network Security Policy

# Alexander Burns, Michael Burns, Dominic Cellini

Our goal is to develop a real-world network security policy that follows and adheres to all current guidelines and standards. The campus has is quite large, and is serving secure policies for over 16,000 students and faculty. Among this large group, we are focusing on six colleges on campus, three management offices, and an on-premises IT department. One of the main goals, since the 2020 pandemic, is to ensure that all students and staff who have the ability to be remote can do so with top security and integrity. This mainly includes, but is not limited to, those who have a contagious illness or those who cannot attend due to transportation issues or inclement weather. Ensuring the health and safety of our campus, as well as securely and properly using our campus networks, is our goal.

We are implementing a five-step policy to ensure the maximum and most efficient cybersecurity policy. This includes identifying, protecting, detecting, responding and recovering.

**Identify**

* Access Control
  + Authentication
    - Students will access the network in two ways: remote access or by physically being on campus.
    - If students are going through remote access, they will need to utilize the university’s Cisco VPN with valid login credentials.
    - Using SSO, if the VPN credentials are correct, students will not be prompted to login again.
    - Duo Two-Factor authentication will prompt a second verification method.
    - If students are on campus, and attempting to access network resources, they will first need to be connected to the campus WiFi, and accept the valid certificate, as well as provide valid logon credentials.
      * Utilize WPA3
    - When on campus, each building will have a different range of IP addresses. Based on what IP address DHCP assigns to the device will indicate which building the student is in and allow the student to access the servers.
    - There only way physical authorization would be a student ID card to access certain rooms, and to use RamPrint.
  + Authorization
    - When students connect to the college server either through the VPN or campus WiFi, they will only have certain privileges lower than that of faculty or IT staff.
    - Privileges include being able to read only, read and write only, and full access which will allow the user to remove, move and read and write any files or directories.
    - In some cases, with limited access, a password is required to perform certain actions (move, remove).
    - When accessing the college website on the server, there would be no further authentication than logging in with credentials and Duo.
      * All resources that are on the website should be accessible to anyone who can access the server.
  + Access
    - Physical access control includes requiring keycard access to enter the building.
    - Certain rooms required elevated access (i.e. electric room, storage room, IT server room, reservable conference rooms).
    - Information security policies include proper authorization, such as secure passwords, VPN’s for securely accessing networks on campus.
  + Acceptable Use
    - Not exploiting vulnerabilities for malicious or personal gain. Submitting a ticket to the IT department instead ensures proper use of technology use.
    - Only downloading and running software that is approved by the university.
      * Best case scenario is to use RamCloud for most application-specific software to courses.
    - Connecting only up-to-date devices that have the most recent, secure, and least vulnerable software.
      * WiFi will be upgraded to the most recent standard: WiFi 6. Devices that do not support this connection standard are most certainly not secure and nowhere near up-to-date.
    - Not using IT resources for personal, unauthorized uses that result in capital gain or profit income.
    - Tampering or accessing unauthorized IT resources or department resources is strictly prohibited and will come with fines and expulsion.
    - Use of unauthorized/confidential information in a malicious way.
    - Adhering to only viewing legal content on the internet (i.e pirated music/movies are STRICTLY prohibited).
  + Security Training and Awareness
    - Starting by making an informative and persuasive short article that all students and faculty will have to read about the money and dangers involved in poor knowledge of cybersecurity attacks.
      * This is in hope to bring light to the ongoing and high concentration of cyberattacks of larger organizations.
    - Before anyone gets a domain account, they will have to successfully pass a course on cyberattacks, including how to recognize them, how to avoid them, and how to notify the IT department about these attacks to spread awareness.
    - Make sure that maintenance staff, as well as outside contractors who work on campus premises have the most up-to-date IoT devices before connecting to elevated privilege network for faculty and maintenance staff.
      * Reference to the Target hack where hackers were able to break in via the HVAC companies’ insecure IoT temperature devices connected to the main network.
    - IT will send out phishing emails throughout the semester to random groups of faculty and/or staff. Those who fall for the email and click the link will be on the most restrictive access until they pass a phishing attack seminar and test. Upon successful test grade, the user will have to change their password, and reauthenticate to the network, as well as network resources associated with their domain.
    - IT will notify all faculty and staff of most recent cyberattacks relevant to victims of similar size to our organization. Emails will include a short and concise summary of the attack, how it is executed, and how to avoid and mitigate the attack.
    - IT will use specific software to monitor any and every threat that comes across the campus network.
    - IT will produce and finalize a group policy that gives access and restricts the scopes and abilities of each group.
* Identification and Authentication
  + Ensure that all users have proper naming schemes:
    - Students have first two initials followed by a 6-digit ID number based on enrollment date at WCU, followed by “wcupa.edu”.
    - Staff and other faculty have the first name initial followed by last name and “@wcupa.edu”.
  + Information systems implement multifactor authentication for all accounts attempting to access and modify college resources.
  + Verify that a device is authorized before establishing a connection to the network.
    - If the certificate is not signed, or credentials are not valid, deny connection until these conditions are satisfied.
    - This is a great area for a network DMZ to be implemented.
  + All users and their registered devices must reauthenticate to the network every 30 days.

**Protect**

* Credentials
  + Usernames of student accounts will follow a set format, with the student’s initials followed by his/her ID and the school email suffix.
  + Passwords will be required to have at least 12 characters.
  + Passwords will be changeable through a common portal secured with HTTPS.
  + Entry of the old password will be required to set a new password.
  + If a student forgets the old password, he/she will have to provide another form of identification.
  + If a student has provided his/her credentials to any site identified as phishing, he/she must reset the password as soon as possible.
  + Passwords authorization will have a certain number of attempts before the account is locked out, and the IT department will have to manually unlock the account and reset the password.
    - Having a lockout for incorrect password attempts significantly minimizes the probability of successful brute force attacks.
  + Passwords must be reset every 90 days to a new complex password that is not similar to the previous and is not the same as any other users on the network.
* Remote Access
  + For accessing on-campus servers remotely, connecting with the university’s Cisco VPN will be required.
    - Use of the VPN should be limited to university-specific needs.
  + Apps and services from third-party providers will be accessible remotely via their respective external servers. These servers will have their own security policies, but the IT Department should be notified in cases where security issues arise.
    - If such security issues are severe and ongoing, an alternative service should be implemented as a replacement.
* Network Integrity
  + Access points should be placed around campus in locations least vulnerable to damage or theft.
  + Access points should operate under a common SSID for students and faculty with WPA3 Enterprise Security. Credentials should match student accounts.
  + Guest access should be limited to a separate SSID secured with a captive portal. This network should also be available to student devices that do not support WPA3 Enterprise if they have been whitelisted individually by MAC address.
  + The admin console should not be accessible outside of administrator systems.
* Physical Media
  + Systems should be configured such that executables on physical media, such as flash drives and external storage drives, do not automatically execute upon insertion. This is usually labeled as “AutoRun.”
  + Systems should be configured to reject bootable installation media on boot. Otherwise, the installed OS may be vulnerable to data loss or corruption.
  + Physical media should be stored in locations with controlled access to prevent potential tampering and data loss. Ideally, these locations should also be climate-controlled to maximize the life of the media.
  + Physical media that is no longer in use should be properly sanitized. Only then can it be disposed of or transferred to different ownership.
* Software Patches
  + System updates should be installed regularly on all systems.
  + Patches for security issues of high severity should be applied within a week. Doing so is crucial to defend against potential attacks.
  + Patches for security issues of low severity should be applied within a month. This ensures that there is adequate time to evaluate the quality of said patches before they go into effect.
  + A system on an operating system revision no longer receiving patches must be enrolled in an extended support program. Otherwise:
    - A full system upgrade to the latest revision will be required, or
    - The system must be disconnected from the Internet.
* Encryption
  + Faculty computers should be secured with full disk encryption. This is to prevent unauthorized access to private information stored on the system disk.
  + Full disk encryption should be paired with UEFI and a Trusted Platform Module.
  + Traffic in remote access to the university network should be encrypted. This is provided by the Cisco VPN.
* Personal Data and Information
  + Student and faculty data should be stored on university-provided cloud storage whenever possible, such as Microsoft OneDrive or Google Drive.
  + Active, unlocked computer systems should not be left unattended to prevent unauthorized access to those systems and the data they carry.
  + Emails should be checked for the sender address, subject line, text, and spelling/wording before opening any attachments or clicking on any hyperlinks.
    - Hyperlinks should also be checked for any attempts to mimic an original, known website. Failure to do so could result in unintended sharing of credentials with an attacker and subsequently, unauthorized access to the associated accounts.
    - If unsure about whether an email is genuine, students and faculty should ask someone they know about the email in question.
  + Students and faculty should be cautious about sending any personal information via email, even if the recipient is known.

**Detect**

* Continuous Monitoring
  + Ideally, this includes:
    - Mobile device monitoring using MDM solutions to configure the security policies of the device. Routinely scanning devices for malicious links or code.
    - Processes to check for upgrades or patches to software components.
    - Checking access control features such as passcodes or biometrics.
    - Detecting anomalies with the device such as malicious code or policy violations (e.g. passcode outdated, passcode too weak, biometrics turned off, auto updates turned off).
* Antivirus Software
  + Antivirus software should be installed and enabled on all faculty systems. Students are encouraged to do the same on their systems.
  + Virus definitions should be kept up to date to keep up with the newest malicious software.
  + System scans should be configured to run regularly to look for active threats and quarantine them before they can cause damage.
* Logging
  + All network equipment on campus should be configured to generate logs of network activity that are stored securely.
  + Any critical errors and suspicious activity logged should be forwarded to the IT Department for swift evaluation.
  + Log storage should be monitored to ensure that it does not exceed capacity and prevent potentially crucial activity information from showing up for later reference.
  + Log access must be restricted to network administrators, as unauthorized access could expose personal information.

**Respond**

* Responding to Security Incidents
  + Responses should be handled by a designated team in the IT Department.
  + The team will investigate the specifics of incidents, including the cause or causes, damages, affected people, and time window.
  + If an incident is linked to the security of a third-party service, the team will cooperate with the provider of the service to have the issues resolved.
  + The team may access student logs and records if necessary to carry out an investigation into any incident.
  + Affected people should be contacted via email to notify them of how they were affected and the steps they can take to stay safe.
  + Depending on the severity of the incident, a comprehensive plan may be devised to prevent future occurrences of a similar incident.
* Planning for Future Responses
  + The effectiveness of the most recent responses should be actively monitored to decide where improvements need to be made.
  + Response plans should not be disclosed or changed without approval from the security team.
  + Plans should be updated according to the changing security landscape. New security threats need to be accounted for in these plans as soon as protections become available.

**Recover**

* Implement and use software that will allow the IT department to detect, perform analysis and any suspicious activity on the network.
* If an incident were to affect the network, that area will be quarantined until the attack is most definitely cleared and there is nothing lingering from it.
* That affected portion of the network would then be put under the most restrictive policies, and put on another IP segment from the main network.
* Our priority in a time like this is to ensure the smallest amount of damage and data leakage occurs.
* Backup images of servers, routers and other network devices will be taken every night, and each individual image will be stored for 45 days before being archived.
* Thorough documentation of the setup for each college, management building and IT department will be thoroughly and clearly documented. Ethernet wiring will and wall jacks will be labeled and documented.
* There are 3 levels of incident threat levels: low, medium and high
  + Low incidents would include low scale, minimal impact attacks such as phishing emails. This would be low since, if properly trained, students and faculty would be able to tell they’re faulty and avoid clicking on them. In good practice, a ticket would be submitted to the IT department and the campus would be notified of the attack.
  + Medium level threats include attacks in the realm of small-scale DoS attacks, mainly flood-style attacks. These include SYN-flood, UDP flood, ping flood and SYN flood. If any of these attacks are successful, comprehensive action will have to be taken, but in no way should the entire network have to be quarantined.
  + High level threats are the most serious and invasive attacks, and immediate action must be taken. Attacks will have an impact on daily studying for students and operations for faculty. The highest level of security and quarantine is required. These attacks include leaks of significant data, threat actors being able to access and give themselves escalated privileges, and large DDoS attacks that shut down the entire network.