Mackenzi Dellolio

March 13, 2025

ITS Desktop Support Group

Old Dominion University

CYSE368 - Spring 2025

Contents

Introduction

The decision to pursue an internship with Old Dominion University's ITS Desktop Support Group was motivated by my desire to bridge the gap between academic knowledge and real-world application in the cybersecurity field. As a senior in the B.S. Cybersecurity program at Old Dominion University, I've spent time developing theoretical knowledge, but I recognized the importance of gaining practical experience to truly understand the complexities of cybersecurity. One of my professors emphasized the value of starting at the help desk to master the foundational skills essential to any cybersecurity career. This internship, under the guidance of Charlotte Kimbro and Matt Sorecelli, allowed me to gain firsthand experience and solidify these core skills.

During my internship, I had four main learning objectives that helped guide what I wanted to focus on. First, I wanted to understand how Intune and Entra (Azure) are used to control who can access devices and what software they can use. Before this internship, I didn't have any hands-on experience with these tools, so getting the chance to work with them helped me see how important they are for keeping systems secure and organized. My second goal was to learn about security policies and compliance. I was especially interested in how rules are set and enforced when it comes to things like administrative rights or installing software. My third objective was to understand how the team finds and fixes security problems, such as software bugs or devices that aren't secure. I got to see some of the tools they use to check for vulnerabilities and learned how they respond when something is flagged as a risk. This helped me connect what I learned in class to what actually happens in a real IT environment. Lastly, I wanted to understand how device asset management works throughout the entire life cycle. This includes everything from setting up new devices, managing them during use, and properly removing them when they're no longer needed.

This paper will reflect on my internship experiences, from the initial training and orientation to the projects I worked on and the lessons I learned. I'll discuss how my academic coursework prepared me for the challenges I faced and how on-the-job experiences reshaped my understanding of the cybersecurity field. By connecting my learning objectives with real-world applications, I will examine how the skills and insights gained during this internship will influence my remaining time at Old Dominion University and my future career path in cybersecurity.

Beginning of the Internship

The organization providing my internship is the Information Technology Services (ITS) department at Old Dominion University (ODU). This department is part of the university's Division of Digital Transformation and Technology. ITS at ODU is a vital part of the university's infrastructure, supporting its technological needs across the entire campus. Its core mission has been to support the university's evolving digital needs. This includes providing technical assistance, managing software and hardware, and ensuring that all IT systems run efficiently to meet the university's objectives. The primary service ITS provides is IT support for the entire university. This includes troubleshooting issues related to user accounts, hardware, software, and network services. ITS also assists with moving computer stations to new office spaces, managing software installations, and maintaining secure and functioning workstations for all members of the ODU community. Additionally, ITS utilizes the ServiceNow system used for tracking and resolving trouble tickets, which is an essential tool for providing efficient IT support. ITS at ODU serves a wide range of users, including students, faculty, and staff across the university. The department's customers are part of the broader higher education demographic, which includes individuals from diverse backgrounds. The department focuses on supporting the entire university community, ensuring that all technological needs are met and troubleshooting any issues that arise.

My first impression of ITS at ODU was one of surprise at how large and organized the team was. I didn’t realize there were several specialized groups within ITS, each focusing on different areas of IT support. I was introduced to the Desktop Support Group, which handles most of the trouble tickets for various buildings on campus. My orientation included a tour of the IT offices around campus and an introduction to the full-time personnel. The training I received was hands-on, focusing on Intune, the platform used for managing devices, and ServiceNow, the system used for submitting and tracking trouble tickets. This training has been crucial in helping me understand how to assist in resolving IT issues effectively.

Management Environment

The overall management and supervision structure has been well-organized during my internship to ensure interns receive the proper guidance and support needed for their roles. The Supervisor, Charlotte Kimbro, oversees all student workers, including myself. We have easy access to Charlotte through Microsoft Teams, where a dedicated student worker chat is updated daily with the tasks we are expected to complete. This helps create a sense of accountability, ensuring that every intern clearly understands their responsibilities and the projects they are working on.

In addition to Charlotte’s supervision, each intern works closely with full-time employees who help guide them through their day-to-day tasks. In my role at the Ellmore College of Health Sciences building, I report directly to Matt Soricelli, a full-time employee who assigns trouble tickets submitted via the ServiceNow system. The ITS Desktop Support Group also uses several Microsoft Teams group chats that allow interns to contact other full-time staff members for any questions or clarifications. This collaborative environment ensures that any questions or uncertainties can be addressed promptly, promoting an open line of communication across the entire team. This consistent communication ensures a strong support system, allowing interns to feel confident in their tasks and responsibilities.

The management environment at ITS has been incredibly effective in fostering a positive and educational internship experience. The support provided by both Matt Soricelli and other full-time employees has been essential in helping me develop my skills and knowledge during my time here. For instance, Matt has ensured that I have received adequate training on critical programs and software, such as NetDisco, CrowdStrike, and Intune, which are integral to ITS operations. His effort to make sure I have access to the proper resources and personnel for learning and troubleshooting has developed my ability to handle various tasks confidently.

Throughout the internship, I have appreciated the level of independence I have been given. As a self-starter, I thrive in environments where I can work on tasks independently, and the flexibility to do so has allowed me to take full ownership of my responsibilities. For example, when faced with unfamiliarity with the detailed steps required for specific trouble tickets, I utilized resources like scripted procedures provided by the ITS Desktop Support Group to help guide me through the process. These resources guided me on how to approach each task while also allowing me to develop my problem-solving skills. However, I never felt left to figure things out independently. The support system within the Desktop Support Group is strong, with easy access to supervisors and full-time staff whenever I needed assistance. I never hesitated to ask questions, and the quick responses from the team ensured that I was never left feeling stuck or overwhelmed. This combination of independence and support has been invaluable to my personal and professional growth.

Overall, the management environment at ITS has allowed me to learn and grow at my own pace while being supported every step of the way. The fact that I've learned to navigate procedures independently, such as packaging software or handling specific troubleshooting steps, means that I am becoming more adept at managing my tasks, a skill that will serve me well in my future career. The internship experience has not only exposed me to a wide variety of technical tools and practices but has also equipped me with the skills to find solutions independently, which I believe is invaluable in cybersecurity and IT

Work Duties, Assignments, and Projects

During my internship, I was responsible for several daily tasks that contributed to the efficiency of the IT department. One of my daily tasks was monitoring ServiceNow for new support tickets and ensuring they were addressed promptly. Additionally, I kept track of the student worker chat in Microsoft Teams to stay informed about any new tasks requiring immediate attention. Another key responsibility was maintaining the cleanliness and organization of the IT shop, ensuring that equipment and workspaces were ready to support operations.

Throughout my internship, I worked on various projects that benefited my building, the faculty, staff, and students in my building, and department. These projects ranged from troubleshooting and resolving IT issues to assisting with hardware setup and maintenance. One significant project occurred in the Ellmer College of Health Sciences Building, which houses the dental clinic. ITS received a trouble ticket regarding malfunctioning mouth camera tools, and the task was assigned to me. After troubleshooting, I identified that several computer stations had outdated software and required an update to Mouthwatch. Since updating 36 devices manually would be inefficient, my co-worker Matt and I decided to package the software update and deploy it through Intune. This ensured that all devices, including any new ones added in the future, received the latest software version. A detailed account of this project is included in Appendix B.

Additionally, I assisted with faculty device replacements in the Health Sciences Building. My responsibilities included preparing new devices, ensuring they were properly enrolled in Intune, updating them to Windows 11, and documenting user information for inventory tracking. I also helped faculty members transition by reminding them to back up important data and ensuring necessary software installations. Once a device was replaced, I wiped the old device, labeled it with the wipe date, and coordinated with property management for proper disposal. A work sample demonstrating my experience with asset management can be found in Appendix A.

In the IT shop, I encountered various troubleshooting scenarios. One customer brought a USB drive that worked on their Mac at home but not on their Windows office computer. After researching, Mac machines can format USB drives to be Mac-exclusive. I reformatted the drive to be compatible with Mac and Windows, resolving the issue. Another instance involved a faculty member who needed to print from their work laptop. I ensured their device was connected to the VPN and added the necessary printers, noting that this method only works for faculty and staff accounts.

These hands-on experiences strengthened my technical troubleshooting skills and problem-solving abilities. They provided valuable insight into common IT challenges and effective solutions, preparing me for future roles in IT and cybersecurity.

Use of Cybersecurity Skills

Before starting my internship, I had classroom and lab experience with cybersecurity concepts, such as understanding common threats like phishing, malware, and ransomware. I also had a foundational knowledge of security best practices, including the importance of strong passwords and software updates. I learned about network security, firewalls, and VPNs through theoretical exercises in classes, but I had no hands-on experience in this area. Additionally, I was familiar with general cybersecurity tools like antivirus software and intrusion detection systems.

I gained practical experience with specific cybersecurity tools and techniques during my internship. I learned about patch management and its importance in keeping systems secure. One of the key skills I developed was using NetDisco to monitor the network for new devices. I learned that any unsupported devices that connect to the network are flagged as a security risk, which is crucial for maintaining network integrity. Additionally, I gained a better understanding of VLANs (Virtual Local Area Networks) and their role in securing sensitive data. For example, the dental clinic in the Elmer College of Health Sciences building uses a VLAN to comply with HIPAA regulations. If there were a violation, the responsibility would fall on ODU. In contrast, the pediatric clinic uses a hosted platform where the hosting company is responsible for security and HIPAA compliance.I also gained insight into disaster protocols, learning that ODU uses an "Alertus" system to push warnings to products connected to ODU through Intune.For example, when an alert is sent out, a notification pops up directly on the computer screen (see Appendix A, Figure A1). I also got hands-on experience tracking and managing IT security tickets using ServiceNow and monitoring security alerts.

This internship significantly expanded my understanding of cybersecurity. I gained a deeper insight into how cybersecurity is implemented in a real-world environment, particularly concerning vulnerability management, network security monitoring, and regulatory compliance. I learned the importance of proactive measures like monitoring network devices and updating systems with patches to prevent security risks. Moreover, my exposure to HIPAA compliance and the use of VLANs for securing sensitive data gave me a better understanding of how organizations protect privacy in healthcare settings. The experience with disaster protocols, specifically the Alertus system, highlighted how organizations ensure safety and communication during emergencies. This internship helped me appreciate the importance of continuously evaluating and addressing potential vulnerabilities and maintaining effective disaster response systems.

ODU Curriculum vs. Internship Experience

The education I received at ODU laid the groundwork for the technical skills I applied during my internship. My coursework, especially in network security and command prompt usage, helped me understand core concepts like VLANs, patch management, and system monitoring. For example, while I had learned about VLANs in class, encountering them in a real-world setting allowed me to better understand their role in securing networks, especially in healthcare environments where HIPAA compliance is a factor.

One class that proved especially helpful was my Windows Management Services course. It gave me valuable experience using the command window, which I used frequently during my internship to configure and load new devices into Intune. My previous coding experience also helped me in this area, since I was already familiar with syntax structure and how command-line environments work. That background gave me a stronger foundation for troubleshooting errors and understanding how different commands interact with the system.

The internship also exposed me to tools and procedures not covered in class. I learned to navigate ODU’s trouble ticket system and gained experience with real-time problem solving, communication, and multitasking in a professional environment. I picked up practical knowledge, like how ODU uses specific command prompt syntax for configuring devices. One small but important lesson I learned was the difference between "\" as a file path and "/" as a command switch—something that helped me avoid errors when setting up systems.

Overall, the internship helped me see how classroom learning applies in real-world settings. It helped me connect technical knowledge with practical tasks, and it boosted my confidence in applying these skills outside of an academic environment..

Assessment of Learning Outcomes/Objectives

Objective 1. Intune/Azure: Understand the use of Intune and Entra (Azure) as it relates to access control for device usage and software.

The internship provided my first hands-on experience working with Microsoft Intune and Entra, which were not part of my classroom education. Through practical tasks and guidance from my mentor, I developed a foundational understanding of how these tools are used to manage and secure devices within an enterprise environment. I learned to use Intune to enroll and manage new and existing devices and how Entra is used for managing user identities and controlling access to university resources.

I learned to use Intune to manage devices, configure settings, and support the university's security standards. One of my primary responsibilities was enrolling new devices into Intune, which included assigning them to the correct user and applying the appropriate settings and policies. I also used Intune to monitor device status and ensure access control was properly implemented. For example, if a user needed access to specific university-licensed software, they could be added to the appropriate group, granting them access. I also learned how Intune can package and deploy software to multiple devices at once, saving time and ensuring consistency across the organization. This was especially helpful in environments like the dental clinic, which has around 36 managed devices.

A specific software in Intune I learned about during my internship was MakeMeAdmin, which allows temporary admin rights for software installations. Users are granted 30 minutes of administrative access only if they meet specific requirements. Their device must have a designated primary user in Intune, and they must be added to the "MakeMeAdmin" group. To be added to this group, users must complete and route the necessary paperwork explaining why they need administrative privileges. This process is a key part of the organization's access control strategy. It enhances security by ensuring only authorized users can gain temporary admin access, allowing the IT team to trace accountability. If an unauthorized or malicious program is installed, the approved user is responsible. Additionally, the feature will not even appear to users who have not completed the proper steps, reinforcing security protocols through conditional visibility.

While Intune plays a significant role in managing devices and access locally, Microsoft Entra works alongside it to provide broader identity and access management across the university's cloud systems. Microsoft Entra is key in managing user accounts and devices. Whenever someone logs into an Office365 application, Entra links that login to the used device. Supported ODU devices are easily identified within Entra by a blue tag, which helps IT staff. To be considered an ODU-supported machine, a device must be enrolled in both Entra and Intune. This is how the system distinguishes between a university-owned device and a personal one. Intune is primarily used for physical device management, such as tracking compliance and enforcing settings on actual machines. Entra, conversely, is a cloud-based system that controls access to university resources by managing identities, logins, and group memberships. Together, these systems provide layered security and centralized control over who can access what and on which devices.

Additionally, Active Directory (AD) is used to manage access to on-premises resources such as network drives and shared folders. Being part of certain Intune groups or AD groups determines whether a user can see or access specific drives. For example, Active Directory allows system administrators to give someone like Matt access to the K: drive but only to specific folders. One challenge in transitioning from on-premises Active Directory to cloud-based systems like Entra is setting up specific folder-level access. Because of this, ODU continues to use both systems side by side.

My mentor, Matt, explained that while other organizations might use different cloud-based management systems, many concepts—like identity-based access, policy enforcement, and centralized device management—are consistent across platforms. This insight made it clear that becoming comfortable with Intune and Azure met this internship's learning goal and prepared me to work in environments that use similar tools. Overall, the experience deepened my understanding of how access control is implemented in real-world settings and highlighted the importance of centralized management in maintaining organizational security.

Outcome 2. Policy and Compliance: Understand security policies and compliance as it relates to administrative rights and software.

During my internship, I learned about several security policies at ODU related to administrative rights and software compliance. One example was the policy requiring faculty and staff laptops to be connected to the VPN and logged into a faculty/staff account in order to access printer networks. Students are not allowed to connect to these networks to help maintain security.

I also gained valuable experience with patch management procedures. The IT staff uses a standard email template to notify faculty and staff when a patch is scheduled to be deployed. The message advises users to back up their data and serves as a paper trail in case the patch causes issues, such as system crashes or software errors. Each month, an Excel sheet is released outlining the patch schedule. It includes details on which device groups will receive the patch, the deployment dates, and information about the patch itself—such as whether it relates to Microsoft 365 or other software.

Microsoft releases patches to ODU, and from there, IT staff can manually schedule the deployment. This flexibility is important because some updates may cause compatibility issues with critical systems like the VPN or antivirus software. By scheduling patches ourselves, we can test them in advance and ensure a smoother rollout with minimal disruption to users.

Outcome 3. Detection and Defense: Understand the tools used to detect vulnerabilities related to devices and software.

The internship contributed to my understanding of detection and defense tools by exposing me to NetDisco, which monitors the network for new devices and flags unsupported ones as potential security risks. This tool, along with the security monitoring practices in place, helped me recognize how vulnerabilities are detected and mitigated through proactive network monitoring. Additionally, I learned about ODU's reporting system for phishing emails and scams, including fake job advertisements sent to faculty, staff, and sometimes student emails. This system is important in identifying phishing threats and helped me further understand how organizations respond to and manage cybersecurity risks.

Outcome 4. Asset Management: Understand the life cycle of device asset management including on-boarding, management, and off-boarding.

During my internship, I gained valuable insights into the full lifecycle of device asset management. I was involved in the onboarding process, where we added new devices to Intune and configured them to meet the organization's security standards and ensured proper tracking and identification. As part of this process, we added the device's primary user, their MIDAS ID, and information about the device's location, such as the building and room number. This ensured that each device was configured correctly and accounted for regarding user responsibility and physical location, which helped streamline future management and troubleshooting.

During the lifecycle of a device, it is managed primarily through Intune, which includes tasks such as pushing patches and updates and adding devices to specific software groups. Intune helps ensure that all devices remain up-to-date and compliant with the university's security standards. In addition to Intune, we also use ServiceNow, our trouble ticket system, to manage issues reported by users. Whenever a user encounters a problem with their device, a ticket is created in ServiceNow, and the issue is tracked and addressed. This system allows us to monitor and resolve device-related problems efficiently.

When devices were decommissioned, I assisted with the offboarding process, which included labeling each device with the date it was removed from service. This label allowed us to easily track which devices were ready to be sent to Property Control for disposal or repurposing. Additionally, we followed strict security protocols when offboarding, including wiping all sensitive data devices, removing them from Intune, and ensuring they were physically secured until Property Control handled them. This hands-on experience helped me understand the critical role asset management plays in maintaining not only the performance of devices but also in protecting the organization from potential security risks and ensuring compliance with institutional standards.

Motivating Aspects of the Internship

The most motivating aspect of my internship was the potential opportunity to apply for full-time positions upon graduation, provided I performed well as a student worker. This possibility inspired me to put in my best effort, knowing that it could lead to a rewarding career opportunity. Additionally, the internship offered endless opportunities to learn and gain experience. The more I was willing to learn and take on, the more I could explore different aspects of cybersecurity and IT, which kept me excited and motivated throughout the experience.

I was also motivated by the people I worked with, especially Matt, who has been incredibly knowledgeable and supportive throughout my internship. His willingness to teach and guide me made a big impact on my learning and confidence. The IT Desktop Support Group team also stood out to me because they work together seamlessly, always helping one another and making sure everyone is taken care of. Their supportive team environment, combined with their encouragement of professional and personal growth, such as making sure staff take advantage of educational benefits, made me feel like I was part of something meaningful.

Discouraging Aspects of the Internship

One of the most discouraging aspects of the internship was when things got slow, and there weren't many opportunities to complete trouble tickets. During these times, I felt like I wasn't fully using my skills or contributing as much as I wanted to. It was frustrating to feel like I was just waiting around instead of learning or helping.

Additionally, at the beginning of the internship, I felt a little discouraged because it seemed like I might not get the chance to learn much about the cybersecurity side of things. A lot of the early tasks were focused on basic desktop support, and I wasn’t sure if I’d be able to explore the security-related topics I was really interested in.

However, over time I realized that there were still ways to learn and grow—I just had to take the initiative. When things slowed down, I started reaching out to other departments to ask questions about their systems or processes. I also took the opportunity to visit other IT shops on campus to see how they did things. This helped me stay engaged and continue learning, even when there weren't immediate tasks. It also showed me that sometimes you have to look for your own learning opportunities instead of waiting for them to come to you.

Challenging Aspects of the Internship

One of the most difficult parts of my internship at ODU was learning the specific systems and software used by the university, especially in specialized areas like the dental clinic. The scale of the systems at ODU was significantly larger than what I was used to. For example, in a typical dental office, there might be 2-8 computers running at the same time, but in the ODU dental clinic, there are 36 stations, each with 2 monitors. In addition, the clinic uses over 700 pieces of software to support its operations, which made troubleshooting and understanding the setup especially challenging.

I also had to familiarize myself with MATLAB, a key software used by the dental clinic, in order to provide better support when dealing with trouble tickets. Prior to my internship, I had no experience with this software, and learning its functionalities was essential to identify potential solutions to technical issues they were facing.

To overcome these challenges, I relied heavily on my mentor, Matt, who was already familiar with the dental clinic's systems as he had helped set them up. I regularly turned to Matt for guidance, asking questions and observing his troubleshooting process. He helped me gain a deeper understanding of both the software and the clinic's overall setup, allowing me to gradually become more confident in handling technical issues related to their systems.

Recommendations for Future Interns

For future interns, the most important preparation is to put yourself in an open mindset. Be ready to learn new things, as each building on campus (depending on where you're placed) comes with its own set of challenges. For example, the Arts & Letters building has its own unique set of systems and issues, just like the Oceanography & Physics lab. Each location specializes in different types of software, and the machines used in those buildings often require specialized knowledge to troubleshoot. Keeping an open mind and being adaptable to these specific challenges will help future interns navigate the diversity of systems they'll encounter during their internship.

To succeed in this internship, it's important to be proactive and ask questions whenever you're unsure about something. Whether it's a specific system or troubleshooting process, reaching out to colleagues, especially your mentor, will help you quickly build your knowledge. Also, take the time to observe how your mentor or team members handle issues and requests. By paying close attention to their strategies and best practices, you can apply those lessons to your own tasks. It's also essential to invest time in learning the software and systems you'll be working with. The more you familiarize yourself with these tools, the more confident you'll be when tackling technical problems. Staying organized is another key factor; with so many systems and tasks, keeping track of trouble tickets, issues, and solutions will help you manage your workload effectively. Finally, remember to embrace the learning process—challenges are part of the journey, and the more you push yourself to understand new systems and tools, the more rewarding your experience will be.

Conclusion

One of the most valuable lessons I gained from my internship was the importance of adaptability. Each building and department at ODU has its own unique systems, software, and challenges, and being able to learn and adapt quickly was essential to successfully contributing to the team. I also learned the importance of collaboration and asking for help when needed. My mentor, Matt, was an invaluable resource, helping me understand the more complex systems and guiding me through troubleshooting processes. Finally, staying organized and proactive allowed me to keep track of various tasks and manage my workload effectively, which helped me navigate the busy and fast-paced environment of the internship.

This internship experience has profoundly influenced my remaining time at ODU. It has given me a clearer understanding of how IT systems function in a university setting and how different departments rely on specialized software. Moving forward, I plan to use this insight to better manage my studies and consider how IT systems apply to my academic work. Additionally, I will seek out more opportunities to work with hands-on technologies, as I now understand the importance of gaining practical experience alongside my coursework.

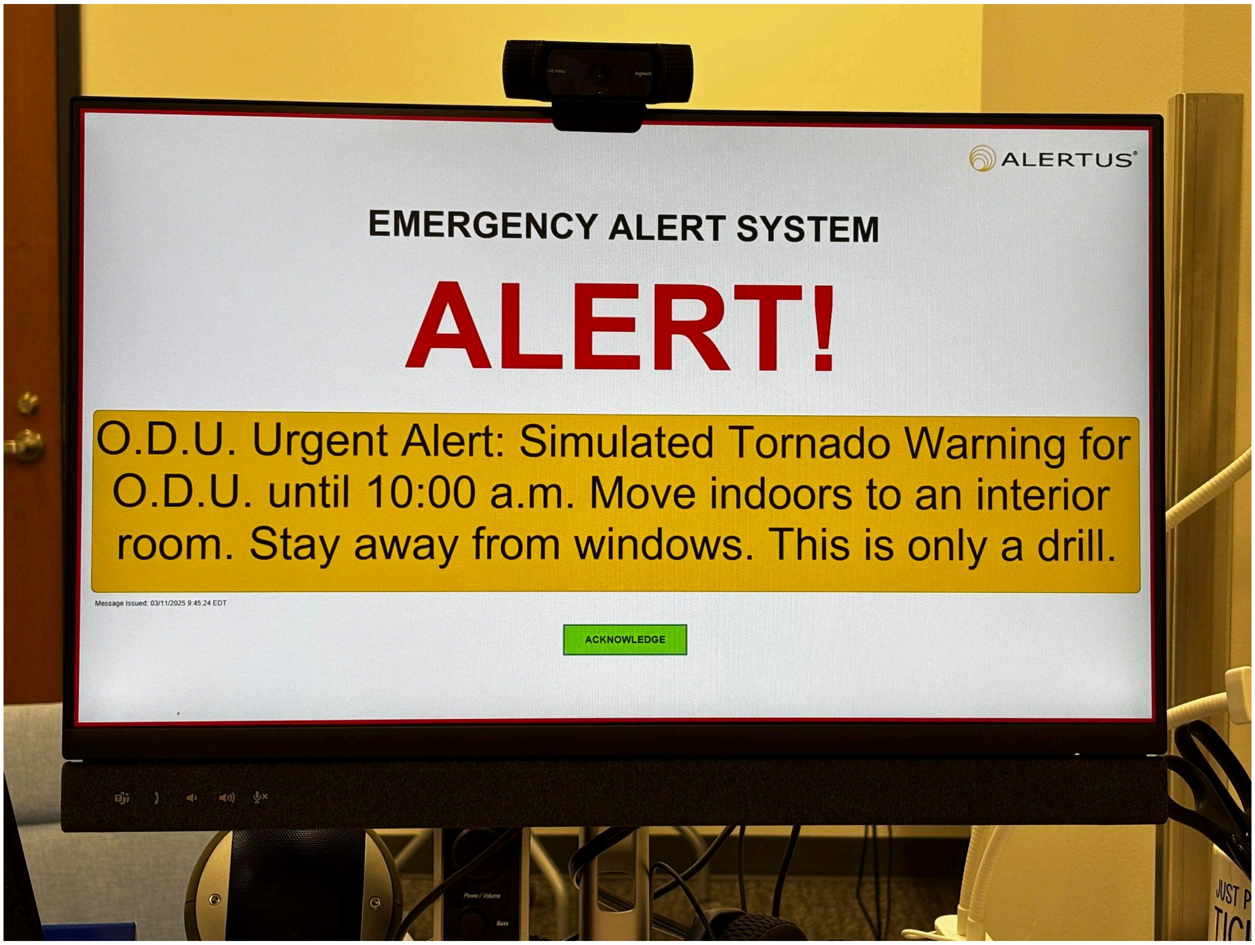
This internship has significantly shaped my career planning. The experience not only deepened my technical skills but also reinforced my interest in pursuing a career in IT support and systems management. Understanding how different departments utilize technology has sparked my interest in specializing in support for specialized systems, such as those found in healthcare or education. The hands-on experience with troubleshooting and working with diverse technologies has also given me more confidence in my ability to contribute to future professional roles. Overall, the internship has given me a clearer direction for my career path and motivated me to continue building my knowledge in this field.

Appendix A

AlertUs Notification Example

Figure A1

Photo taken by author during internship.



EMERGENCY ALERT SYSTEM

ALERT!

O.D.U. Urgent Alert: Simulated Tornado Warning for O.D.U. until 10:00 a.m. Move indoors to an interior room. Stay away from windows. This is only a drill.

Message Issued: 03/11/2025 9:45:24 EDT

Appendix B

Work Samples from Internship

Work Sample 1

ITS received a trouble ticket that the mouth camera tools in the dental clinic were not working correctly, and the ticket was given to me. After going to the clinic to troubleshoot and determine the issue, I realized that some computer stations had out-of-date software and needed Mouthwatch to be updated. Since 36 devices would need an update, it seemed inefficient to go individually. My co-worker Matt also mentioned that it is essential that any new machines would receive the latest version of the software. We decided to package the software update and push it out to all the devices through Intune. This was the most efficient solution, and it would also ensure that any new devices added to the Dental Clinic would get the latest version of the software. During this process, I learned how to package an EXE file into something Intune can understand. I created a temp folder on my C drive and then made a folder called Mouthwatch. In the Mouthwatch folder, I included the Intune application file. In a folder labeled 2.7, I included the updated download for Mouthwatch. I then used the command line to create a file that Intune can read and use to push out the software update to the device group. Once I had all the files, I uploaded the Mouthwatch folder to the MEM deployment folder in Teams. I created a task for MEM deployment to push the update to the Dental Clinic device group.

Work Sample 2

At ODU, the typical life cycle of a device is five years, with the clock starting when the device is received, not when it is first used. In some cases, devices may remain in their boxes for extended periods before being assigned to users, which means that the user only gets three years of actual use. The five-year life cycle is based on the device's warranty period, which is standard upon purchase. Understanding this time frame is essential for effective asset management and ensuring that all devices are accounted for properly, as it also helps in anticipating how many devices will need to be replaced soon, allowing us to manage our time and resources better.When preparing a new device for a user, my first task is to ensure that it is correctly enrolled in our cloud management system, Intune. This step is essential for managing the device remotely and ensuring its security. Additionally, I must make sure the device is updated to Windows 11 and that all relevant user information—such as the device's location, the assigned user, and the serial tag—is accurately recorded in Intune. This process is essential for tracking the device and inventory purposes, ensuring that assets can be easily accounted for.Another part of my role involves assisting users with transitioning to their new devices. I remind them to back up their OneDrive and other vital data to avoid data loss. I also ask if they require additional software, ensuring their new device is added to the appropriate Intune groups for installation. The most straightforward part of the process is connecting the new device and verifying that all software and settings are correctly configured.Once the new device is set up, I take the old device back to the IT shop. I begin by wiping the device to remove personal data and labeling it with the date it was wiped for future reference. The final step involves working with the property management team to ensure the proper disposal or recycling of the old device.