CYSE 368 Internship Final Paper

Ramzi Alkaifi

Earth Viability Center, Inc. / Place4Us

Employer/Supervisor: Dr. Hans-Peter Plag

Instructor: Professor Charles Kirkpatrick

CYSE 368 / Internship

Fall 2026

Date: November 2026

Table of Contents

1. Introduction 3
2. Management Environment 4
3. Major Work Duties, Assignments, and Projects 5
4. Use of Cybersecurity Skills and Knowledge 7
5. How the ODU Curriculum Prepared Me 9
6. Learning Outcomes and Objectives 9
7. Most Motivating or Exciting Aspects 10
8. Most Discouraging Aspects 11
9. Most Challenging Aspects 12
10. Recommendations for Future Interns 12
11. Conclusion 13

Works Cited 15

1. Introduction

I did my CYSE 368 internship at the Earth Viability Center, Inc. (EVC) and the Place4Us platform. CYSE 368 is the cybersecurity undergraduate program at Old Dominion University, and the internship allowed me to take the knowledge I had acquired in courses and transpose it to a real platform.

I found this internship through the CYSE 368 requirement and the possibility to work with EVC on cybersecurity research for Place4Us. According to the signed Memorandum of Agreement (MOA), my internship at EVC was called "Cybersecurity Expert", where the MOA declared I would have Hans-Peter Plag as my internship supervisor and that my work at the internship would focus on cybersecurity issues useful to the organization.

Place4Us by the Earth Viability Center EVC is a 501(c)3 nonprofit registered in Virginia, working toward a future in which human needs are met, and the Earth's life support system is protected. EVC's Place4Us is one of our core services. Place4Us is a social collaboration platform built on Virtual Community Centers or VCCs. EVC's VCCs enable communities to organize, share information, reflect, consider, collaborate, and work on issues that matter to them. While the platform is designed to serve communities, it does not provide a commercial social media experience. Since a Place4Us platform comprises users, communities, files, profiles, participation and other forms of engagement, privacy and cybersecurity are considerations.

My first 50 hours differ from what I do at work or school. When I am doing a normal class assignment, I am given instructions, a question and an answer, or a specific set of results I am to find. During my internship I was given general parameters to research, and I had to learn the functionality of the platform before I could figure out what questions were relevant. For the first 50 hours I mostly read and explored the pages of the site, looked through various VCCs, viewed profiles, admin pages, and looked at the admin area, trying to understand how these various areas fit together.

This was sometimes frustrating in the beginning as I was wary of exploring these areas without knowing what I was looking for. As I learned more about the platform and had conversations about it with my supervisor and other interns, I learned better what questions I should investigate.

My first training was directly on the platform and the internship itself, which was an online internship. I learned how the structure of VCC worked, how to navigate Workspace areas, how the user and admin area were accessed, how files and privacy settings appeared to users, and how the group would communicate and log in progress. We also had meetings and check-ins where we could ask questions and check in on progress and areas that would need more research. This was different from someone physically next to me all day explaining what I was working on, so I needed to learn to become more independent in organizing my research.

My MOA signed off by my mentors laid out four major learning goals I would strive to accomplish during my time here. First, I would review the currently envisioned Place4Us user authorities and roles for the range of users and make suggestions for updates. Second, I would

investigate potential problems associated with the file upload features of the MyFiles system, and other Place4Us components. Third, I would research approaches for detecting images and video created with the help of Generative Artificial Intelligence (GAI) tools. Fourth, I would examine the currently envisioned system for protecting user privacy while maintaining enough discoverability for users and their content. All four of these challenges were integral to the work I was doing. I would focus on the user role and authorities, doing my biggest work on User Roles and Authorities, while continuing to research the other three areas.

As my internship progressed, my work naturally extended these objectives. My research of roles and authorities led to access control, least privilege, administrative authority, security logging, and encryption-key access. My research of privacy led to account cancellation, data retention, discoverability, login tracking, and activity logs. As I looked through the platform, I noticed PHP errors that printed out technical details of the system. Towards the end of my internship, a real-world Place4Us data-loss incident led me to research backups and recovery. These new areas of research did not stand alone from those I initially outlined. They confirmed to me that many areas of cybersecurity are interconnected and answer the same questions of who has access, what can they do, and how is it monitored and documented.

2. Management Environment

A typical working environment for an internship is usually physically on-site at a place of work, which was not the case here, as the internship was virtual and research based. My internship was overseen by Dr. Hans-Peter Plag, and he would give me feedback about how the research was going. Rather than being given many small tasks to do exactly as they were laid out, he often gave me a cybersecurity question or an aspect of Place4Us to research more thoroughly, in which I would then have to navigate the platform, investigate the matter, write up a report about the findings, and either ask questions or provide suggestions back to the group.

The internship included collaborating with the other student interns. We had some overlaps in our research as well as some specific work areas of our own. My primary individual area was User Roles and Authorities, with User Privacy, MyFiles, and GAI Detection being sites of overlaps. Meetings were useful as a forum for us to share what we had learned, to check to see that we were not doubling our efforts, to request help, and to determine what to investigate next. The fact that the internship was done in virtual space meant that communication had to be precise.

I made the best use of supervision when a piece of feedback gave me clearer insight into what happened in Place4Us. For instance, one of the biggest pieces of clarity I got was that there are platform level authorities, and there are VCC level authorities. A platform authority would be assigned by the system administrator, a VCC authority would be assigned by the VCCs' admin. An authority that worked in one VCC would not necessarily work in another one. This clarity altered the direction of my research: I stopped thinking only about a list of roles, and started thinking about scope, assignment, review, and removal of authority.

The management also matched how we built Place4Us. EVC keeps the platform running and maintains it, but each VCC can be independently administered and governed. This meant that my cybersecurity research could not just look at one set of administrators; I had to consider the

difference between one platform administrator and an administrator within a specific VCC. It turned out that the management environment was good for a research internship; I needed to work without excessive supervision, but I also received the support and discussion of my group members when I needed help.

3. Major Work Duties, Assignments, and Projects

My big take on was the User Roles and Authorities. I started in the VCC Administration pages but looked at the Registered Users pages in other VCCs, people's profiles, governance areas, my Workspace, privacy settings, and the People search. I was looking for where a user in a particular role could see that role and authorities and how those concepts were laid out. There was some role-related information in the Registered Users pages, such as name, email, position and affiliation, and location, but I did not see a place where a user's specific Place4Us role and authorities was clearly presented. I also learned that a position listed on a profile should not be automatically assumed to be a Place4Us role because it could be a position outside the platform.

It was made clear that access control could not be based solely on user identity. It was also necessary to understand what a user is authorized for and where that authority was applicable. I went back to previous research from Place4Us on access control, which listed several roles that had been considered for the platform. As the research I was using was from 2025, I treated this more as research starting point rather than assuming these roles were still being used in the same manner.

I also researched different areas including role-based access control, least privilege, authentication, authorization, separation of duties, and privileged access. I was able to map out the authority process and authorization criteria as Request Approval Assignment Use Activity Logged Review Removal. I produced a draft Roles and Authorities report and matrix, which organized the research into a more usable form for developers rather than a set of disconnected notes.

User Privacy was yet another important task. I looked over the privacy settings, discoverability, account deletion, login data, activity data, and links remaining to the data. On the account deletion data, the write-up simply said that some contributions made may be published, which makes the data user privacy lifecycle come to mind: why is account data collected, who has access to it, what happens if it is no longer needed, and what information will be retained. I then looked at data deletion and thought about privacy as a cycle. It is never enough to simply ask whether information is collected. We need to ask, why do we collect this information, how is it to be used?

Another element of privacy work was activity logging. Security logs can be beneficial in tracking potentially malicious activity, unsuccessful login attempts, administrative activity, or activity in general that can be considered for review. However, as well as this, activity logs also capture data about the users themselves. My advice was not to do away with security logging but rather to specify who can view the logs, how they are secured, the length of time the logs are kept for, and whether any significant administrative action is being recorded. This was valuable to Place4Us as security logs are only beneficial if they are being stored securely, and access is limited.

I checked the file access levels for MyFiles that were available to the user – Private, Members, Users, and Public. My main problem here was that there was no information on what these would imply, on the page itself; from a new user's perspective, when considering whether to upload or share a file, knowing who can see what you upload is important. I made some suggestions for descriptors of the levels, and as an aside, other ideas for organizing files – bookmarks, favorites, and user-created folders. MyFiles was important as some of the sharing that occurs on the site involves creating privacy and access-control issues, when users are not aware of what they are uploading.

GAI Detection was a collaborative project. By that point, the team already knew several potential signals that indicated that an image, video, or text was generated by AI. Instead of just adding a few more signals, I thought about what needed to happen after a signal was spotted. I designed a process whereby content is submitted, potential AI signals are checked, further confirmatory evidence is gathered, a human looks at the evidence, a final decision is reached, and the result is recorded. The key detail was that a single signal should never be accepted as conclusive. Missing metadata, strange image characters, writing style etc. could all be warning signs, but those issues could also arise in a human-generated piece.

I also looked at previous Place4Us work on encryption and password security. My supervisor asked how users could be prevented from reusing their old passwords. I found that this did not mean keeping the old passwords in a readable and reversible format for that purpose. You can test the password history by storing password-verification values in the database in a way that does not have to be reversed to verify the password. This led me back to related work on Roles and Authorities because the encryption key is a similarly sensitive resource. I asked which users should be able to change the encryption key and suggested that the scope of that access should be kept as narrow as possible.

While I was browsing the site, Place4Us, I encountered errors all over the place such as within the Action Items page, The My House page and the admin/handlers (governance pages). Some of the errors even included internal server file paths, filenames, and line numbers which contained PHP errors. This was an example that was not in a textbook; I was witnessing it live on the website. My recommendation was that general users should see just a simple error message, but the relevant technical error information should be written to internal logs (only accessible to developers).

At the end of the internship there was a data-loss event where some of the internship reports and other data were lost, including two of the reports I had written earlier. This gave me a real reason to research backup and recovery and I designed a recovery plan that tracked the cause of the loss, prevented additional changes, identified what was lost, identified the appropriate backup, put the information back, checked the information was correct, notified the users who lost data, documented the data-loss event and enhanced safeguards. I also suggested having more than one usable backup, backing up the data frequently, testing restoration, protecting backups independently, and restricting high-impact deletion or data-replacement operations to specific administrators.

The projects were essential to the organization, because Place4Us is still in development and real communities are using it. The research did not always lead to a discovery confirming

vulnerability. Often the useful output was identifying an ambiguous thing, observing and recording what I could see from a naïve user perspective, researching the security principle behind the observation, framing that into a question or recommendation that developers can evaluate, and communicating it. As such, I can support the organization with an external cybersecurity lens to aspects of the platform that include users, permissions, privacy, files, logging, AI content, and restoration.

A key component of accomplishing these tasks was also writing up what I had done, to be examined by others. I kept track of all my research, produced various progress reports, reflected on my work, and created a more narrowly scoped User Roles and Authorities report. My writing of the reports allowed me to check whether I really was drawing from my observations when I drew those conclusions. It also made me aware of ways in which I was conflating things. For instance, a user position, a platform role, and a technical authority are similar-sounding entities, but they are not interchangeable. Authoring the report allowed me to sort out what that difference was and explain how important it was.

I also learned that a recommendation has to be tailored to the platform, not simply re-stated from a cybersecurity manual. Most individuals understand that least privilege is a good rule of thumb, but what does that mean for Place4Us? Does the authority apply for the entire platform or only one VCC? Who can assign or ask for it? How does the user request it? What happens when the user no longer needs it? What does that mean for privacy and logs? It wouldn't make much sense to just have a recommendation to get rid of the logs simply because they had user info on them, rather, it makes more sense to not allow the logs to be accessed or kept when they have no value. I found that as I went along, I was asking these questions for every project I did.

4. Use of Cybersecurity Skills and Knowledge

Prior to the internship, I already knew some cybersecurity material from my ODU classes. I learned more broad concepts like authentication and authorization, network security, access control, encryption, password security, threats, and protecting sensitive data. However, I came to see how those were used during the internship. In class, the problem is defined, and you know the question that you are answering. During the internship, I needed to figure out what the question was before I could research it.

Most obviously: access control. My understanding of the principle was that anyone should have as few permissions as they could. On Place4Us, I needed to figure out how to implement that idea on a platform that required both platform- and VCC-level authority. I learned how to think in terms of scope: authority applies to an entire platform, a single VCC, a particular group, a single workspace, or a particular resource. I also learned to look at the lifecycle of an authority: permissions are not just granted; they are requested, approved, used, logged, examined, and revoked.

My view of privacy has also evolved. Prior to this internship, I knew that privacy could be a matter of how data was mishandled, but I was concerned with secrecy more than with privacy. During the internship I began to write increasingly nuanced questions about what privacy meant in this context. Why are we collecting this information? Do we need all of it? Who can access it?

How long do we keep it? What happens if we cancel an account? Can the user limit the discovery? How do we ensure our security logging information is private? And so forth.

Secure password storage was one of the areas where I initially applied knowledge that I had gained previously and then expanded that knowledge. I was aware that passwords should not be stored in clear text. The question asked in my internship about storing old passwords caused me to think a little about password history. The purpose of stopping a user from reusing old passwords does not require retaining clear text versions of their old passwords. Securely hashing passwords will allow the reuse to check to compare new passwords to the stored value rather than the actual old password.

Secure error handling and information disclosure were valuable lessons learned from the PHP errors. A more innocuous example can be found in the classroom demonstration; disclosing the path to a file might seem like a straightforward bug. But this is exactly what I experienced on Place4Us, just by using the site. That made the lesson real. We will of course want detailed errors to our developers, but the exposed detail to the user should be minimal. This links with logging as the details will be available in the log file, just not on the screen.

The data-loss experience opened my eyes to the backup and recovery principles. The concept of backup seemed so straightforward before the internship: take a copy of all data so that it can be recovered if needed. I realized then that a backup plan is just a part of the entire process. The backup should be recent, safe from failure, and functional. There should also be a reporting process in place. Backups and restores are both technical and managerial processes.

Additionally, I strengthened research and communication skills that are relevant for cybersecurity. I learned to separate out things I directly experienced and those I was speculating about. For instance, when I could not see a role or general authority, that did not necessarily mean the site lacked an internally established authority system. It only meant I had to record what I could see and inquire if there might be other checks on the system at the admin/developer level.

The internship taught me that the disciplines of cybersecurity are not isolated; they are all about systems. They all tie together into a system – roles and authorities relate to privacy, because they determine who is allowed to view data; they relate to logging, because permissions imply access and execution; they relate to backup and recovery, because anyone with power must have restrictions; they relate to encryption, because someone must be in charge of the keys.

One skill I learned during my internship was how and when to stop and ask for help. At first, I would have tried to answer a question by only looking at more pages. Then I learned to write down what I had discovered and to be specific about what I was still missing to make my life easier, for example by distinguishing between the two levels of platform and VCC authorities. Finding the simple answer to my supervisor's questions about the two levels meant I could adapt to the structure of my research.

Something else I learned is the human element of security decisions. Something can be technically secure but confusing for the user. MyFiles showed that because the access options may be meaningful on a technical level, but the user has to know what Private, Members, Users,

and Public means before making a choice. This also applies to the privacy and account deletion settings. A policy or setting is much stronger when the user can make that decision at least to some degree of understanding. I have been considering usability more when I think about computer security instead of only considering security as a technical setting.

5. How the ODU Curriculum Prepared Me

My cybersecurity courses at ODU gave me the terminology and the security fundamentals to comprehend the internship. I learned enough about the fundamentals of systems and network security in the courses to comprehend why authentication, authorization, access control, encryption, and security principles were important, including the principle that you can't trust a user just because they've logged on. They also provided me with the practice of reading technical articles, analyzing security issues, and justifying a control rather than naming the control.

Some ideas I learned in school became more real during the internship. At least privilege became less abstract when I had to imagine what actual authorities required. Password hashing became more real when I considered what if old passwords were stored on the server. Secure error handling became more real when I encountered real PHP errors with server information. Backup and recovery became more real when we lost data. The examples in the assignments became more real when our org could really use the research.

Coursework also assisted me in the research component of the internship. It is common in cybersecurity to compare a system to security practices and show how a recommendation is valid. My writing and policy classes assisted me in structuring data, incorporating sources, and translating my research into documents that another person could evaluate, which I had to do with the User Roles and Authorities report and the 150 hours of research I assembled afterwards.

This semester also gave me a taste of what a course cannot. Most notably, ambiguity was the most different part. In class, I usually knew the goal of the assignment. At Place4Us, I sometimes had to learn whether what I was seeing was a security hole, a design decision, a piece not yet implemented, or if I was missing some context. I had to ask questions and adjust my beliefs in response to feedback. That was by far the most valuable aspect of this internship because real cybersecurity work often does not start with a clearly defined problem.

These skills included a variety of softer skills. I had to learn how to write my hours, track research, document my progress, and communicate with those working on the platform in a manner that could be easily read and applied to improve their work. These skills are tied into my education because it is worthless to find a technical weakness if it cannot be communicated to others. The internship experience opened my eyes to the fact that my ODU education opened many doors, however, I must be able to use judgment and communicate effectively with others to be enormously successful.

6. Learning Outcomes and Objectives

My first goal was to analyze the current model of the wide variety of user authorities and roles on Place4Us and suggest ideas for improvements. This goal turned out to be my largest project

and was accomplished more thoroughly than any other goal. I examined several areas of the platform to determine where users, administrators, roles, and authorities appeared. I clarified that there are both platform-level and VCC-level authorities, and that powers granted in one VCC are not automatically granted in another.

I read previous research in access control, created a roles-and-authorities matrix, formulated a series of questions that still needed to be answered, and suggested an authority's lifecycle. A report documenting all of these ideas was then written and provided to the Place4Us team. I learned that authority must be clearly defined, scoped, assigned, reviewed, and revoked.

My second goal was to investigate potential problems with the plethora of options for uploading files under MyFiles and other places in Place4Us. I completed this goal by looking over the various places in Place4Us where file access options are available, especially Private, Members, Users, and Public. My primary concern was that this page could better indicate what option one should choose to keep certain groups from viewing one's file. Also, I considered how user-made options, such as bookmarks, favorites, and user-created folders could be set up in ways that would make storing information easier to organize. This goal is related to privacy and permission because the security of files is not only based on technical access guidelines, but the account holders' knowledge of them.

The third of my goals was to look at how we might detect an image or video that has been generated with Generative Artificial Intelligence tools. This was a collaborative task, and some flags were devised that could be examined when viewing images, video, and text as well. I focused more on what we do when we detect a flag for which a decision needs to be made. I concluded that one flag should not necessarily be a signal to assume the image/video was generated with generative AI – there may need to be further checks before a decision is made, and human review. I proposed a pathway from submission to a potential flag to further checking, then final human review, then decision and recording. This taught me about false positives and the risk of making a moderation/security decision based on just one sign.

My fourth goal was to examine the current draft for compliance with protecting user rights while maintaining enough user and contribution discoverability. I accomplished this by examining privacy options, discoverability options, deleting accounts, activity logs, login data, and data storage questions. I found that Place4Us offers privacy options but I would like to see more explanation around what is saved when you delete your account (specifically about what gets deleted, what might be saved, how long it is saved, whether any data is anonymized, etc.), explain in more detail what is stored as activity logs and determine who can view them, and consider privacy issues in logging activities, with controls around access, storage and protection, and retention time.

The four objectives were not separate. Roles and authorities meant one person's classified information may be accessible to another. MyFiles got us thinking about permission and knowledge. GAI got us thinking about evidence, review, discretion, and decision. Privacy got us thinking about logging and access. After my time at the internship, I saw these four objectives as related points of one big cybersecurity issue: what should a platform be able to know about a user? Who should the user be? What should the user be able to access? What should the user be

able to do? What information should the platform log? What information should the platform share about the user?

Working back through the objectives together also demonstrated to me that I progressed from exploration to analysis. In the first 50 hours of the internship, I primarily sought to understand the platform and trace the problems to the functionality of the supported administrative areas. In the second 50 hours, I streamlined the research and began to prepare reports, questions, and suggestions. In the final 50 hours, I was connecting the original objectives to password security, error handling, logging, encryption-key access, and backup and recovery. To me, this progression matters because it means that the internship was much more than a set of different standalone tasks; I gained experience with the platform over the course of those 150 hours.

The goals also clarified where additional work might be possible, without that additional work counting as part of my essential hours. Some inquiries relied on information known by administrators or developers, but not users, and I could not access it. My job in the internship was to report what I could observe, find out about the cybersecurity concern, and carefully articulate what still needs to be validated. That can be an adequate conclusion because a cybersecurity investigation may not yield a "yes or no" result, but a clear statement of the unresolved question.

7. Most Motivating or Exciting Aspects

What was the most exciting part of the internship? The most exciting thing about the internship was that I was able to identify something from the live system and then leverage it in the realm of cybersecurity. The PHP error was a perfect example because I did not have to picture an imaginary system to learn about. I could visualize internal files and processes as they were happening in real time and then dig in to understand how a user-facing error message should be treated.

The data-loss event was similar. Backup and recovery seemed more intriguing after I had seen what happened when data was lost.

I was also happy to see my Roles and Authorities work come into a clearer picture over time. In the beginning, I was mostly just clicking from one page to another, trying to understand what I was looking for. Later I was able to go ahead and make a process, a matrix, some questions, and a recommendation. When I received the comment that my Roles and Authorities report was worthwhile, I felt connected to the platform instead of just working on something just to get a grade.

The other encouraging part was finding similarities in all areas of cybersecurity. At first, I had tasks assigned to me, but eventually, access and authorizations linked everything I researched together. That made the internship more real, as a real platform would not split into course chapters like that. Privacy, passwords, files, logs, backups, and encryption all impact each other.

8. Most Discouraging Aspects

The most disheartening aspect of the internship was uncertainty at the start. I am used to being given an assignment that explains exactly what we are looking for, so being told to research a section of a large platform left me unsure what to do. I often feared that I was spending too much time browsing pages without generating enough meaningful output. It was a while before I realized learning the system was part of the work and that I needed to learn about the system before I could make cybersecurity recommendations that made sense.

The data loss was also disheartening as some of the work was lost, including two of my previous progress reports. It is frustrating to have work that has been done lost, especially when reports are being used to keep track of my internship hours and my progress. Nonetheless, it has become a tangible cybersecurity experience as it provided me with a practical reference for backup and recovery, administrative precautions, and incident reporting.

Another frustrating thing was that I could not always verify the answer to a question from the regular-user side of Place4Us. Not seeing whether an authority was present or how it was represented did not give me a definite answer about how it worked internally. It was something I would have liked to be able to conclude through my research. This was known to be the case in regular-user research, but it was still frustrating not being able to find a definite answer.

9. Most Challenging Aspects

The hardest part was finding my way to research a built system without rushing to assumptions. I had to clearly differentiate between things I saw myself and things I expected to be otherwise. For Roles and Authorities in particular, a profile might document a person's position, but not necessarily document that the individual held that position as a technical role. A VCC Administration page might document a list of sites administrators but not necessarily document all their authorities. I had to learn to write findings thoughtfully, and to transform ambiguity into honest questions.

And then there was the issue of how much research is enough. The areas in cybersecurity are getting larger. Researching one area of a role could turn into authentication, authorization, least privileged access, logging, separation of duties, and account lifecycle. Researching privacy could turn into retention, discoverability, consent, deletion, and logging. I had to keep the research Place4Us-specific rather than be stuck on writing a cybersecurity paper about everything.

The environment on placement was similar in that I had no supervisor watching me throughout the day in an office. I had to keep notes, prepare reports, attend meetings, and decide what to do next. This was difficult at first but with time I learned to enjoy this independence; in the last 50 hours I was far more comfortable with the platform and was able to concentrate more specifically on security and privacy issues.

10. Recommendations for Future Interns

The first thing I would suggest future interns do before working on recommendations is to look at how Place4Us is put together. There are VCCs, Workspace areas, profiles, administration pages, governance areas, file features, and hundreds of other features to get familiar with. If you are unfamiliar with how all the parts work, you can spend a lot of time trying to figure out what a page or a field does. But I also recommend taking decent notes so that initial exploration does not turn into random searching.

Future interns should understand what an observation, question, and confirmed security problem is. There is an observation if a normal user cannot see a role. One should try to ask a question about how the role is stored or displayed, instead of immediately asserting that the site does not have a role system. This will help produce more accurate and useful reports for developers.

It would be good for future interns to have at least a small knowledge of access control, authentication and authorization, password hashing, privacy, logging, and backup concepts. They do not have to know all the answers but at least if they know the definitions, it will be easier to identify what they have to look up. Also, the intern should be used to read technical articles and compare sources.

Communication is a further key to preparedness. Interns need to be able to communicate in normal language what they have discovered, ask questions if a requirement is not clear, and begin sharing work with other interns. Since there are some cross-over topics, excellent communication can avoid unnecessary duplication of work by multiple interns. Interns should also keep a back-up of important reports and notes, so their work is not lost if a file is accidentally removed.

And I would add one last piece of advice. I would remind future interns that some of the best work does not come to us as a ready-to-go to school project. The best work might start with a vague question. The intern might have to poke around the platform, get the lay of the land, do some research into the cybersecurity concept, and then figure out which recommendation is appropriate. Be patient with that process and keep everything organized, and the internship will be much more manageable.

Interns in the future might want to take this further and use feedback to improve work completed previously, rather than seeking to make each weekly task completely standalone. Some of my most significant learning came from revising previous submissions when I received a clarification and was able to revisit a published observation, change my interpretation, and update the report – which is crucial on a developing platform, where features and concepts may evolve during the course of the internship.

I would also advise that future interns organize their work outside of a single spot on Place4Us. The data-loss incident taught me how essential it is for research, progress reports, and drafts to have backups elsewhere. I do not say this just as a suggestion for Place4Us, but also as a bit of advice for an intern. If your work is well organized, it will be easier for you to recover work and compare previous research and create your final internship paper without having to remember what you did.

11. Conclusion

150 hours spent working with Earth Viability Center and Place4Us gave me an entirely distinct perspective on cybersecurity than what I am used to seeing in the classroom. I came in at first uncertain of how to approach such a large existing platform without being presented with one specific technical challenge. By the time I left, I felt comfortable navigating the platform, asking cybersecurity and privacy-focused questions, researching those questions, and synthesizing my results into recommendations.

What I learned from the internship is that cybersecurity sometimes is not about a single glaring security flaw. It can be about understanding how something was designed, who should have access to what, whether users have considered their privacy options, whether it logs activity or not, what is the backup and recovery process, and always, asking the question-why? I learned how much access and authority tie these issues together. Privacy is defined by who has access, MyFiles is based on who has access to the files, logging is based on who has access to the records, the backup and recovery process is based on who has the authority to perform important administrative operations, encryption is based on who has access to the keys.

This experience will stay with me for the rest of my time at ODU because I will approach cybersecurity related work more from the standpoint of how I could do this in a real organization. When I research access control, logging, encryption, or recovery, I now have a real platform to relate to. I also now understand the importance of research and communication; a technically accurate idea still must be communicated well before someone else can evaluate and apply it.

I learned that beyond technical software and technologies, the work in cybersecurity is investigation, documentation, communication, and understanding of systems. It was encouraging to see myself become more confident working on my own and with questions that are not easy to answer. And I learned to be wary of how easy it is to confuse what you know with what you think is real. Those are the skills I will use in the future.

As a whole, the internship accomplished the main goals stated in my Memorandum of Agreement and provided me with exposure to User Roles and Authorities, User Privacy, MyFiles, GAI Detection, access control, encryption and password security, security logging, error handling, and backup and recovery. More importantly, I learned how those topics are integrated on an actual platform. The hours I put into my internship allowed me to go from understanding the framework of Place4Us to researching certain cybersecurity topics and providing recommendations based on what I experienced.

Works Cited

Earth Viability Center, Inc. Place4Us platform and internship materials.

Alkaifi, Ramzi. *CYSE 368 Memorandum of Agreement*. Earth Viability Center, Inc., 2026.

Jennings. *Access Controls on P4US*. Place4Us cybersecurity research slides, 2025.

National Institute of Standards and Technology. *Role Based Access Control and Cybersecurity Guidance.*

OWASP Foundation. *Authorization, Logging, and Password Storage Guidance.*

National Institute of Standards and Technology. *Contingency Planning Guide for Federal Information Systems.*

Cybersecurity and Infrastructure Security Agency. *StopRansomware Guide.*