Access Control and Network Security Checklist

ID	Security Control issue	Applicable (Y/N)	Complete (Y/N/NA)	To be Done Priority (High, Mid, Low)	Ease of fix (Easy, Moderate, Difficult, Not Fixable)	Full Description of processes to address issue
1	A cloud based platform is being used for access control with only public available items being readable by general public.	Y	Y	Low	Easy	The cloud platform used is Github which provides controls like read-only permissions and settings to change access controls that account for this issue.
2	The cloud based platform provides for hiding information and this is used to protect sensitive information and code.	N	N/A	Low	Easy	N/A; Note the cloud-based platform does have this functioanlity but it is not needed for the purposes of the project.
3	OS access controls are used to only allow authorized changes to be made to code.	Y	Y	Low	Easy	OS access controls were automatically implemented when the project was created. I, the user, and the admin are the only users that have read and write access.
4	Platform user groups are used to only allow changes to be made to code by authorized individuals.	Y	Y	Low	Easy	The cloud platform, Github, implements the functionality that only collaborators are able to contribute and edit to the repository. At this time there are no collaborators but the functionality is there if needed in the future.
5	Backup Policy is in place and being used.	N	N/A	Low	Moderate	N/A
6	Third-Party libraries used in code are up-to-date and have been checked to ensure no security issues exist.	N	N/A	Low	Easy	N/A
7	Physical Security of actual computer code is stored on is adequete	Y	Y	Low	Easy	The physical security of my personal computer is adequate. I use biometrics to login to my computer or a passcode (which I am the only that knows it). I also have the most recent update of Windows 11. It is to be noted that both Samsung and Windows updates are installed on my device.
8	Accounting: Logging is integrated into the code itself (for exceptions, errors, and user input failures at minimum)	N	N/A	Low	Moderate	N/A
9	Accounting: Process includes logging (tracking of changes, user making changes, access attempts, etc)	N	N/A	Low	Moderate	N/A
10	PKI and other encryption and authentication methods are used to connect to cloud platform	Y	Y	Low	Easy	Github uses SSH certificate authorities to authorize users that attempt to interact with Git through Github. This allows Github to authenticate users through different methods. When interacting with Github through Git, the user is prompted to enter a password or temporary private key. Github also uses 2-factor authentication when editing any important information in a repository.

11	Internal Actor threats are accounted for and policies/planning is in place for these.	Y	N	Mid	Difficult	Some threats are currently accounted for during the SWOT analysis and Risk assessment previously completed. However, there are many others that may not be accounted for as human error, in general, is a threat to the system. However, as I am the only internal actor, it is imperative that I take the proper measures to secure my physical and network security.
12	Standard Unit Testing used	Y	N	Mid	Easy	I currently do not have any standard/automated unit testing for the system, however this is fairly easy to implement. I need to implement some type of testing software that will test some of the different test cases needed to ensure that the software is working properly.
13	Security Testing used (the type varies)	N	N/A	Low	Moderate	N/A
14	The endpoints of the system have been accounted for and secured as much as possible.	Y	N	High	Moderate	Most of the endpoints have been accounted for but have not been properly secured. To address this issue I must do more research as to what those endpoints may be and how I should go about securing them. Then I must secure them.

Questions:

Which of these were accounted for on your SWOT or Risk Assessment and how have you started adding countermeasures for them (or how will you start)?

1, 7, 10, and 14 were accounted for in my SWOT Analysis and Risk Assessment. Some countermeasures that I already implemented is that I have made my physical and network security more adequate. I have installed many updates on my computer since then. Using Github, as my cloud platform is a great advantage in implroving the security of my software. Since Github has good security, by association, my software also has good security. It is to be noted that the software on Github has good security, using GIthub does not necessarily improve the security of my network and devices. The last countermeasure that needs to be implemented is related to the endpoints of the software. It was noted in both the SWOT and Risk Assessment that this is a major issue. One possible solution is to edit the logic of the program to increase security, this would allow for less global variables in the program, more specifically the global variables would not hold a key data store for the program.

Select a High Priority item - why do you consider it "high priority"?

The only high priority item I have is 14, "The endpoints of the system have been accounted for and secured as much as possible." I consider this to be a high priority item because it is the main flaw in the software. Many of the other items have been addressed by using other secure systems and software. This item is also high priority because it is one of the main ways that my software could be hacked. The endpoint has been accounted for but not necessarily addressed which is a big issue. The endpint is vital to the logic of the program, it essentially is the data store for the site, and could be easily exploited since it is not secure.

Select a "Not Fixable" or "Difficult" item - why did you select this value for it?

The only difficult item I have is 11, "Internal Actor threats are accounted for and policies/planning is in place for these." I consider this to be difficult because it is hard to think about all the ways that internal actors can be a threat to a system. Given this context, it is a slightly easier since I am the only internal actor, but it can be difficult to think about all the scenarios that may occur. Not only should they be accounted for, but policies and planning should be detailed to prevent any of these threats from becoming a reality. This process can be very difficult and time consuming, so that is why I labeled it as difficult.