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	High	Moderate	The cloud platform used is OneDrive which comes with built-in security features to restrict access to files within the organization. Only public files will be available with a provided link that contains permission outside the organization.
2	The cloud based platform provides for hiding information and this is used to protect sensitive information and code.	Y	N	Low	Moderate	The cloud platform used is OneDrive which comes with built-in security features to protect sensitive data. However, data handled by the code in this project is not highly sensitive so this issue is not a critical concern.
3	OS access controls are used to only allow authorized changes to be made to code.	Y	N	High	Moderate	The operating system used is Windows 11 or Windows 10. The process of adding restrictions to files may be moderately challenging to account for different versions of Windows or different operatings systems all together. Encryption of the code files may help solve this issue.
4	Platform user groups are used to only allow changes to be made to code by authorized individuals.	N	N/A	N/A	N/A	N/A
5	Backup Policy is in place and being used.	Y	Y	High	Easy	The cloud platform used to backup this project is OneDrive. OneDrive ensures there is a copy of the project in the cloud as well as a physical copy on the computer hard drive. This means there are at least three copies of the project on two computers and OneDrive.
6	Third-Party libraries used in code are up-to-date and have been checked to ensure no security issues exist.	Y	N	Mid	Easy	The third-party library used in the project is the cmath library for C++. This library is kept up to date each time the code is booted up in a development environment. However, security issues with this library have not been investigated.
7	Physical Security of actual computer code is stored on is adequete	Y	Y	High	Easy	The physical computer code is stored on a secure cloud platform (OneDrive) that requires 2-Factor Authentication and a challenging passphrase to access. Both physical computers containing physical copies of the code are located within locked spaces, shut off (when not in use), and require a fingerprint lock or complicated passcode for access.
8	Accounting: Logging is integrated into the code itself (for exceptions, errors, and user input failures at minimum)	Y	N	Mid	Easy	Logging has not been integrated into the code as of the current date. However, implementing error handling and user input failure should be simple to add to the code. A log can be created once methods of error handling are established.
9	Accounting: Process includes logging (tracking of changes, user making changes, access attempts, etc)	Y	N	High	Moderate	Logging has not been integrated into the code as of the current date. However, implementing tracking of changes and user identification when changes are made will be moderately difficult to add to the code as the log may need to be manually maintained.
10	PKI and other encryption and authentication methods are used to connect to cloud platform	Y	Y	Low	Easy	The cloud platofrm used for this project is OneDrive. In order to connect to OneDrive 2-Factor Authentication is conducted by a third-party service and a complicated passphrase is required.

11	Internal Actor threats are accounted for and policies/planning is in place for these.	Y	N	Low	Difficult	A planning document exists for the creation and implementation of the project. Currently there is no policy or planning in place for internal actor threats. Since there is only one author for the project, it may be difficult to create policies for interal actors with malicious intent.
12	Standard Unit Testing used	Y	N	Low	Difficult	Standard Unit Testing has not been implemented in the project. This project may not be complex enough to implement Standard Unit Testing.
13	Security Testing used (the type varies)	Y	N	Low	Difficult	Security Testing has not been implemented in the project. The type of Security Testing required for this project will require further research.
14	Programming language and development software is up to date.	Y	Y	High	Easy	The programming language used in this project is C++ and the development software used is CLion by JetBrains. This software automatically updates when the project is opened.

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)?

My created criteria of keeping the programming language and development software up to date was accounted for in my SWOT analysis as a weakness. I have started adding countermeasures to account for this weakness by ensuring the development software automatically updates at regular intervals. I will start implementing the operating system access controls countermeasure because that will be a useful countermeasure to maintain in case the physical security of the project is compromised.

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

I consider accounting for user changes and the identity of the user who make those changes a "high priority" because if a potentially malicious actor gains access to my code and implements something dangerous meant to harm users, there will be a record of who made this change so they can be held accountable according to the interal actor policy. This accounting is also important in case physical security is compromised because then the malcious actor can be identified by the owner of the device.

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

Two items I selected as "Difficult" are Standard Unit Testing and Security Testing. I selected Standard Unit Testing because I am unsure if any method of Standard Unit Testing can be implemented in this project as it is not highly complex. I selected Security Testing because I am unsure how much, how often, or what type of Security Testing will be necessary for this project to be considered secure.