A blue and white cover with text

Description automatically generated

File Management Plan

The following file management plan has been implemented to ensure that all files are organized and easy to locate:

* **File Naming Strategy**
* All files must be accessible on any macOS device
  + Ensuring files are accessible on any macOS device guarantees that they can be easily retrieved and managed across different Apple computers, promoting consistency and ease of use
* File names will include a combination of uppercase and lowercase letters, numbers, and common symbols
  + Using a variety of characters in file names helps to avoid conflicts and ensures uniqueness, making files easier to organise and locate without duplication issues
* File names will be concise yet informative, not exceeding a 50-character limit
  + Keeping file names short yet descriptive helps in quickly identifying the content of the files while maintaining readability and avoiding truncation issues in file explorers and search results
* File names will follow the camel case convention, with no spaces between words. Spaces will be replaced by capitalising the first letter of each word except the first.
  + Adopting the camel case convention improves file name readability and ensures compatibility with systems that may not handle spaces well, thus enhancing overall file organisation and accessibility
* A blue folder with black text

  Description automatically generatedEvidence:
* **Folder Hierarchy**
* Each folder will have a concise but descriptive name that clearly indicates the contents
  + By keeping names concise yet descriptive, it supports the ease of file searching by shortening the duration of finding a certain/particular file
* To enhance the ease of file searching, there will be no more than four levels of nested folders
  + By having a maximum of four levels if nested folders, it allows the files to be organised enough to easily store and find specific files without becoming a tedious process of searching through multiple folders
* Unwanted files will be stored in an archive folder
  + Unwanted files being stored in an archive folder ensures the separation of files, enabling the user to quickly identify which files hold value/are needed for the SAT project
* Evidence:

A screenshot of a computer

Description automatically generated

File Security Plan

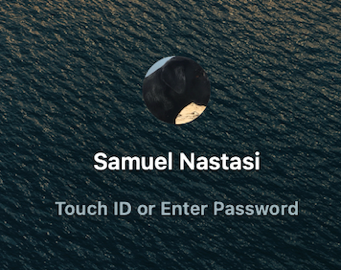
The following methods will be implemented to ensure that all files remain secure and inaccessible to unauthorized parties.

* **Physical**
* **Barriers Techniques**
  + The laptop will be held/stored in a safe and secure location when left unattended
    - The laptop will be safely secured overnight in a space unknown to anyone. This decreases the chances of the laptop being found and therefore stolen.
  + The laptop will be held/stored in an area that is constantly under surveillance by both a large guard dog and cameras
    - Since the device will be kept in an alarm-equipped home, anyone trying to take the data will have to deal with an alert and maybe the authorities.
    - Evidence:

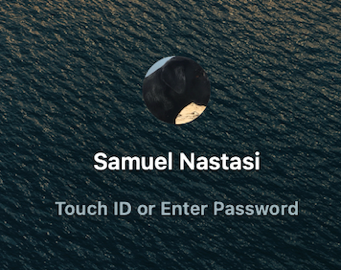
A white wall with a blue window

Description automatically generatedA dog sitting in a car

Description automatically generated

* **Biometrics**
  + The laptop requires fingerprint to be unlocked, as well as a fingerprint to unlock the files
    - In order for an intruder to gain access to the laptop and the files, my fingerprint must be presented, which is extremely difficult/impossible to replicate or steal
    - ****Evidence:
* **Backing Up**
  + All files on the laptop will be copied onto on external drive, which is stored in a secure area with constant surveillance. This area is separate to the stored location of the laptop.
    - By copying the data to another storage device, it allows me to restore and continue my work if the original is misplaced, damaged, etc. This does mean that the drive must be regularly updated to keep the storage device up-to-date with the current files.
    - **A hand holding a black rectangular object

      Description automatically generated**Evidence:

* **Software**
* **Usernames & Passwords**
  + The laptop requires a password to be unlocked, as well as a password to unlock the files
    - In order for an intruder to gain access to the laptop and the files, the password must be correctly inputted, which is extremely difficult as the password is a mixture of uppercase and lowercase letters, numbers and symbols
    - This is used as a basic defence strategy to prevent against unauthorised access from unauthorised individuals
    - ****Evidence:
  + The external hard drive requires a password to be unlocked
    - This serves as a fundamental defensive tactic to stop unauthorised individuals from gaining access.
    - Evidence:

**A screenshot of a computer

Description automatically generated**

* Encryption
  + The external storage device saves all data to it in an encrypted form
    - This allows the data to be transformed into ciphered text, hence increasing the difficulty of accessing the data if the hard drive is taken
    - **A close up of a sign

      Description automatically generated**Evidence
* Firewall
  + The school’s Wi-Fi has a software firewall that filters the traffic coming in and out of the network
    - This ensures security by shielding my computer from malicious or unnecessary network traffic
* System Security Software
  + The computer has a virus detection software that scans storage drives for viruses, worms and more
    - The virus detection software removes, fixes and/or isolates any threats that are identified, saving other files from being compromised