**1.1. Personal Information / Privacy**

All Personal Information is to be:

* + Collected solely for use by NMTAFE
  + Consent must be given in order to gather and use personal information
  + Kept in a secure location
  + Only available to the user and approved users
  + Revived upon a breach and the user notified of the breach

**1.2. Data Retention**

Data collected may include the following:

* + Source and Destination IP addresses
  + Connection information, Layer 4 and Layer 7 protocol.
  + Information contained in packets, regardless of encryption level.
  + Authentication Information
  + Timestamp of connection

This data will be retained for as long as North Metropolitan TAFE see fit and is of use to the organisation. Data will be retained for a minimum of six months after collection until either automatically erased due to storage concerns or manually erased upon request.

The data will be held on premise at North Metropolitan TAFE’s Joondalup Campus physically separated from the rest of the campus with appropriate physical and logical access controls.

**1.3. Acceptable Use**

* + Breach of policy to identify or use data in order to bully/discriminate users
  + All data seen by the analyst is only to be used solely for the purpose of analytics for the security of the organisation

Data that is collected through honeypots contain personal information and traffic specific to different users, this means that the analyst that is analysing the data will see data that may be used to discriminate or bully against users.

**1.4. Intellectual Property**

The digital information collected by the honeypot network will be held by the organisation North Metropolitan TAFE. The information collected belongs to the TAFE, the data does NOT belong to the user after it is collected by the honeypot.

North metropolitan TAFE resides the right to use the data collected by the honeypot the information includes but is not limited to:

* usernames
* passwords
* search queries
* logs

**1.5. Access Control**

* **Who can access the data.** Data that is seen within the Security Operations centre is confidential and access to that data should be controlled and only allowed to be visible to people that it needs to be seen by. GPOs should be used to properly give access.
* **Physical access.** Data seen in the SOC is confidential and should not be accessed by people just walking by, Key card access should be given to a small list of people and only to the people that need to be in there at specific times.
* **Principle of least privilege.** Privilege should only be given to people that need it, you should start with no privileges and move up as you need

**1.6. TDM Security / Network Segregation**

All Honeypots deployed on the TDM Network must:

* Be segregated from the TDM Internal network through the means of Virtual Local Area Networks, different public IP addresses and virtualised docker containers.
* Have all data collected, be encrypted end-to-end

**1.7. Duty to report / SOC Analysts**

Students in the SOC must be due diligent in reporting all wrong doings within the network that is caught by the honeypot.

* Students are subject to report all security breaches, associated vandalism and theft that may occur within the network.
* All data must be reported by students to a supervisor.
* Establish appropriate trust levels to ensure that all data misuse is reported.