Lindsay note: The solution being described in this document is a **proposed** one that has not yet been coded, and so the answers to these questions relate to how the proposed system **will** operate, based upon extensive research of the MyLO/D2L API.

**Infrastructure Hosting**

* Is the solution hosted on premise or by an IaaS?
  + The application solution is hosted on the NeCTAR Research Cloud Service
  + The database solution is hosted on Google Firebase Firestore
* If by an IaaS who hosts the Infrastructure that supports the application?
  + The application solution is hosted on the Tasmanian node of the NeCTAR Research Cloud Service, provided by Tasmanian Partnership for Advanced Computing (TPAC)
* Where is the solution hosted (ie. Australia)?
  + Tasmania
  + Cloud Firestore location: nam5 (us-central)
* Where is the Disaster Recovery component of the solution hosted?
  + The source code for the solution is backed up to source control (Github) and my personal computer
* Is the solution in its own tenant?
  + Yes
* Who manages the Infrastructure OS and applications that support the solution (ie Server Builds including Security Compliance, Patch management, Change management)?
  + Dr Lindsay Wells manages the Nectar Instance with the Infrastructure OS, and the source control for the solution
* Are the infrastructure and applications managed to a Security standard?
  + No
* If so is the infrastructure and/or applications certified to that standard ie. ISO 27001?
  + No, as above
* Are policies available for review, including but not limited to Security Policy, Disaster Recovery, Risk Management, Incident Management etc?
  + No, as above

**Solution Architecture**

* Is the solution that supports UTAS single or multi tenanted?
  + The application solution is intended for UTAS use only. Single tenanted.
* Are the Databases that support the solution shared?
  + No, as above
* If the DataBase that contains UTAS data is shared with other customers how is the integrity of the data guaranteed?
  + N/A
* If the DataBase that contains UTAS data is shared how is the DataBase Schema structured to manage Client Data securely?
  + N/A
* Is the data encrypted at rest?
  + Yes, the OAuth token for each student will be stored in an encrypted format
* Are you required to store UTAS data for a defined retention period?
  + No
* What is the data retention period?
  + N/A
* In what format/s is the data managed in for the retention period?
  + N/A
* Which endpoint protection is used on the servers that support the solution?
* Are architecture documents available?
  + Documentation has been provided

**Security Compliance/Review**

* If certified to a security standard when was the last Certification review performed?
  + No, note that current application is \*proposed\* and not yet developed, so these questions are not applicable.
  + Note that some collaborators on the project are lecturers in ICT Security, and can assist with performing audits and pen tests.
* Are the Infrastructure and Application audited regularly for Compliance to the Security Policy and the documented Security Controls?
* Who performs the Audit?
* Can you provide a copy of the findings?
* Are the Infrastructure and Application pen tested regularly?
* Who performs the pen test?
* Can you provide a copy of the findings?