Task 1

Search MyAbertay for any policies or procedures you can find that are related to Information Security. Do they conform to the security model that we considered in the lecture?

Give your thoughts. There is no right or wrong answer. Provide bullet points (no more than 6).

Security model - CNSS Security Model

Relevant policies found:

- Asset management: control and disposal
- Information classification & handling
- Data protection
- University electronic mail and messaging
- GDPR for Research
- ICT Facilities Regulations for Acceptable Use
- ICT Regulations for Acceptable Use
- Information Security Controls
- ISMS Regulations Acceptable Use
- ISMS Third Party Access
- IT Systems Vulnerability Management
- Outsourcing and third party access
- University Password
- Patch Management
- Personal Data Breach
- Physical and Environmental Security
- Privacy by Design and by Default
- Research Data Management
- System access control
- Third Party Access
- Virus protection and management

Personal thoughts:

- Found a total of 21 policies I feel could be related to Information Security (2 of these were linked as procedures, but the document title was actually given as "policy"). This could prove difficult when considering the "education" aspect of the model, as too much information can cause confusion to system users;
- The documents were not necessarily the easiest to find (this based on navigation to the page found at My Abertay > Student Services > Student Documents A-Z) which further complicates the goals of an effective SETA program. Could this be made simpler by categorising the documents found on this page? It seems nonsensical to have important policy documents mixed in amongst poster templates with no available search or filter;
- Many of the policy documents I looked at followed different layouts and formats, hindering my ability to find the information I was looking for;
- Many of the policy documents I looked at had not been revised for some time - as an example, the Asset Management: Control and Disposal policy authored by the Information Manager and which specifically references an Information Security framework has not been revised since 2015;
- Focussing specifically on the Information Security Controls policy (as this is the policy whose title most explicitly links to Information Security) - there is no mention of confidentiality in the entire document, nor any mention of education for staff or students, nor or of transmission or storage of data. This policy does not appear to adhere well to the CNSS model;
- Focussing on the Information Classification & Handling Policy - there is mention here of almost every element of the CNSS model, and the policy does appear to adhere well to it. This suggests an inconsistency of approach with regards to policy documents being written (when compared to the Information Security Controls policy), which could result in confusion between the differing communities of interest.

Task 2

Consider National Cyber Security Centre - https://www.ncsc.gov.uk. What general information does it give to business about Information Security. Is this general information relevant to all businesses no matter their size or the nature of the business?

Give your thoughts. There is no right or wrong answer. Provide bullet points (no more than 6.

Personal thoughts:

- The NCSC website has been divided into easy-to-navigate areas - it appears to have been designed so that visitors to the site can find information specific to their own circumstances (reflected in the navigation toolbar that allows for browsing based on size of business or topic of guidance), rather than being subjected to a "one-size-fits-all" guidance sheet;
- The categories of business used are consistent with standard business terms, and a simple definition of the category has been provided on their specific pages, ensuring that site visitors can be assured that they have found the appropriate guidance for their specific circumstances;
- The page content has been tailored to suit the assumed needs of the site visitor - when analysing the language and layout used on the page directed at small & medium-sized organisations it is clear the content is aimed at visitors with only a basic understanding of Information Security principles, whilst the page directed at large organisations is much more formal, with fewer links to "starting-point" guidance;
- The guidance links provided on the pages for differing organisation sizes have been tailored for particular scenarios that the organisation size is likely to encounter (e.g. links to device security guidance for large organisations compared to links to "smart" security cameras for individuals & families);
- Thought has been given to businesses of a different nature (e.g. charities and public sector businesses) and specific guidance provided for their circumstances;
- All in all, I found it difficult to find any "general information" provided by the NCSC - it has largely been categorised and marketed towards businesses of differing sizes and natures. The guidance I read appeared to have been sufficiently tailored to individual business circumstances and has been well written using context-appropriate language for the reader.