ISSP Policies of Educational Institutes (NZ vs. AU)

Due Date: 11 August 2024, 23:59
Weight: 3% of the final grade (1% group work + 2% individual work)
Submission: ECS Submission System

Student's full name: Thomas Green

Other group members' full names: Abia John, Patrick Mills, Annie Foote, Mathias Street, Tom Green, Paige Martin

Instructions and Tasks (In-Person Session):

- In groups of four (4), complete the task(s) below.
- Document your answers and **submit it together with your own answers to the individual work**, using the submission system on the course website. Name the document as YOURSTUDENTID.docx/pdf
- **All members will be receiving the same mark for the group work.**

Instructions and Tasks (If You Missed In-Person Session):

- You will need to perform all the tasks and answer all the questions by yourself.
- Document your answers and submit it using the submission system on the course website. Name the document as YOURSTUDENTID.docx/pdf

1. **Group Work [1 Mark]**
   A. Search Massey University and Australian National University (ANU)'s intranet and official web sites**.** Select an **issue specific security policy** from the list below:
      - **Fair Usage of Information Technology Policy**
      - **Password Policy (selected this issue policy)**
      - **Remote Access Policy**

   B. Find the associated policy documents from the institutions' web sites. (Make sure these policies exist in both institutions).

- ANU: Password Policy -> https://policies.anu.edu.au/ppl/document/ANUP_013008
- MU: Password Policy -> https://www.massey.ac.nz/documents/538/Password_Policy.pdf

   C. Read and compare both documents, discuss them in your group and answer the following questions:
      a. Which university entities (e.g. ITS, School managers, departments, HR etc.) are responsible for issuing the policy documents and enforcing the policies?

- Massey University:
   - Responsible: Information Technology Services
   - Prepared by: Chief Information Officer

- Authorized by: Deputy Vice-Chancellor

- Australian National University:
  - Responsible: Chief Information Security Officer
  - Approved by: Chief Operating Officer
  - Contact Area: Information Security Office

b. Are the policies centrally managed?

Yes, both policies cover the whole of each university and access to all university systems:

Massey University:

- The password policy applies to all information systems, information components, and all users working on behalf of the university. Users include staff and students (including, but not limited to contractors, consultants and volunteers, University will use passwords/passphrases to protect user accounts to maintain the security of information. Usage guidelines are in place, so Massey information systems are protected so security is not compromised for that system. Password policy and passphrase policy is equally applied.

Australian National University:

- The ANU authentication policy is centrally managed. It sets out the access requirements for ANU systems such as email, file storage, software, etc. ANU has procedures to ensure appropriate security for all systems, technology, data, equipment and processes which it has ownership and control. This ownership applies too and provides access to known authorized users within the university community as well as network connecting devices authorized for connection that have been delegated/allocated an IP address in the university IP address range. The university's maintenance and control focus on its responsibility to; provide and maintain access to systems and resources for their known authorized users, suspending any known authorized users access as a result of a security concern or policy break, and maintaining and amending minimum authentication standards as appropriate to reflect modern/current information security protocols.

c. Are there multiple policies related to a **single issue** available on **each institution web site** (e.g. two remote access policies on Massey university's website)? Are they consistent? Do they include any policy rules which are contradicting between the two documents?

MU: Device Security Policy:

- https://www.massey.ac.nz/massey/fms/PolicyGuide/Documents/d/device-security-policy.pdf

MU: Electronic Information Access Control Policy:

- https://www.massey.ac.nz/massey/fms/PolicyGuide/Documents/ITS/Electronic%20Information%20Access%20Control%20Policy.pdf

MU: Device Security Policy:

- https://www.massey.ac.nz/massey/fms/PolicyGuide/Documents/ITS/Electronic%20Information%20Access%20Control%20Policy.pdf

Massey has one central ‘Password Policy’. Passwords are further mentioned in Massey’s ‘Device Security Policy’ and ‘Electronic Information Access Control Policy’ documents but not in detail. All information is consistent and does not contradict one another. “User and device identity and password policies will utilize the appropriate Massey University enterprise Lightweight Directory and Access Protocol (LDAP) wherever possible”.

The ’Device Security Policy’ does mention that staff devices should lock after a maximum of five minutes of inactivity. This does not contradict the ‘Password Policy’; however it does add additional details of when the user may need to enter their password. Highlights that university staff using devices to access university information will; (without exception) use a strong password/passcode/PIN enabled to reduce the opportunity for unauthorized access. Passwords and PINS should be kept secure and compliant with Electronic Password Policy. Also highlighted devices must not be left unsecured whether on or off university premises. When unattended the device must be locked and kept secure.

Massey’s central ‘Password Policy’ was last reviewed in Fed 2023, showing that it is the latest version. There are no outdated versions of this policy that are easy to find or publicly accessible.

ANU: Information technology Security Policy:
- https://policies.anu.edu.au/ppl/document/ANUP_000421

ANU: Password Procedures:
- https://services.anu.edu.au/files/system/Step%20by%20Step%20guide%20to%20reset%20identity%20password.pdf

ANU: Password Guidelines:
- https://services.anu.edu.au/information-technology/login-access/anu-id-password

ANU also has an information technology security policy. This policy is higher level and covers definitions of relevant ideas such as passwords and MFA. There is no contradicting information, this policy is more generalized summary of ideas covered in the password policy. In addition to ANU’s main ‘Password Policy’, ANU has procedures available, e.g. a step-by-step guide to reset identity password. Guidelines are also available, for example, tips on choosing a secure password and passphrase are available in identity manager. From these guidelines, the main password policy is clearly linked.

2. Individual Work [2 Marks] – Continuation of (C)

d. How comprehensive are these policies? Do they cover all the issues related to the issue for which the policy was created for? Can you think of three policy rules currently not addressed by each institute’s policy document?

ANU:

- The policy does highlight major components that do need to be addressed in a password policy such as internal (university managed) responsibilities -> maintenance and management of the system as well as external (students and public) responsibilities -> non-disclosure, comply with set management and standards that are externally and publicly implemented. However, there are some policy rules that have not been addressed that would be considered best practice to be prevalent in a password policy. An example of this is enabling 2FA or MFA, which would add an additional layer of security to user and staff accounts. This would be more secure than having typical 'something you know' questions for a user to authenticate themselves. This would prevent or limit malicious unauthorized users or attacks from happening from a third-party attempting to access university information or system. Another example would be password age, which would require the students, staff or public to change their password for their account after a certain period of time from the password creation. This would add further protection for unauthorized access, for example, is a user uses the same password for other accounts online that suffer from a data leak where users passwords become publicly accessible, so the password is now prone to DDoS attacks. Another example is that every password should be checked against a 'blacklist' that includes dictionary words, repetitive or sequential strings that have been prone or have been identified in security breaches, commonly used passphrases or other words/patterns that malicious attackers are more likely to guess.

MU:

- The policy does highlight components that do need to be addressed in password policies and highlights some policy rules that ANU password policy did not address such as MFA. However, there are some policy rules that could be integrated to make the policy and the university's password/passphrase management more robust. For example, (just like ANU) password should be checked against a 'blacklist' that includes dictionary words, repetitive or sequential strings that have been prone or have been identified in security breaches, commonly used passphrases or other words/patterns that malicious attackers are more likely to guess. Another thing the MU policy is lacking is discussion about how user passwords are managed by the system and how they are enforcing that users passwords are remaining confidential. By highlighting more on the procedures and universities responsibilities. The MU password policy does not highlight on any public password legislations or best practices they have incorporated as well.

e. Do these policies reference relevant external standards, laws or regulations? List them!

ANU:

- As mentioned in the authority section of the password policy it addresses multiple external standards, laws and regulations; addresses the Information Infrastructure and Services Rule 2020 that is administrated by the Australian Department of Education (https://www.legislation.gov.au/F2020L01675/latest/versions). Also addresses the Australian National University Act 1991 (https://www.legislation.gov.au/C2004A04206/latest/versions), showing that this policy has is being enforced as a 'must have' by all Australian universities. Also addresses the Public Governance, Performance and Accountability Act 2013 (https://www.legislation.gov.au/C2013A00123/latest/versions).

MU:

- Addresses the Privacy Act 1993, and Copyright Act 1994 to ensure that the document that copyright on the document is not breached and ensure that this document is an obligation for the university to uphold to protect password information from third-parties. Also addresses procedures such as Code of Student Conduct and Acceptable use of Technology policy to make sure that all users of university services are conformed to the appropriate groups.

f. Do these policies target the right audience (users of the technology/system)?

ANU:

- This document/page is more of a procedure than a policy that highlights on how passwords and authentication information is going to be managed by the university and what users of the university system need to conform to use the system appropriately. It however doesn't mention of cover any student conduct policies or staff conduct policies. Its target audience is at students, staff, alumni and affiliates however, but its layout is more or less of a procedure.

MU:

- This document is a policy that has been layed out to highlight on the universities use of passwords as a form of authentication to access the universities systems. This document is affiliated as a point in the student and staff conduct policy for them to adhere to if they wish to use the universities systems and services.

g. How do these two institutions compare with regard to policy non-compliance?

ANU:

- Highlights the universities responsibilities for suspending an authorized users access as a result of a security concern or policy breach which may result in disciplinary or penalty action. Also highlights how to report suspected security incidents such as a compromise of authentication details highlighting that security is both a university and student/staff responsibility. Also provides an email address to students to message if they have any concerns on what to do and if they are worried if they are not complying to the universities password policy.

MU:

- Highlights on if there is a violation of the policy it would result in disciplinary action, termination or legal action if students or staff do not comply to the policy.

What to Submit: Submit answers to the questions under C (max 3 pages) using the ECS submission system by the due date. A comparison table is suggested for improved readability (See table below).

e.g. Remote Access Policy	**Massey University**	**Australian National University (ANU)**
Issues by the same entity?	Yes/no, briefly explain	….
Are there multiple policies related to a **single issue** available on **each institution web site?**	Yes/No, e.g. remote access policy is addressed in "**Remote Access policy**" document as well as fair usage policy document, with contradicting information	There is only one single document ("**work from home policy"**) addressing the remote access procedures and guidelines
How comprehensive are they? List any related missing policy rules	e.g., Massey's remote access policy does not specify the operating systems which should be running on remote clients' devices	ANU's remote access policy does not require clients to use encryption for remote access

Format of the report is single spaced with default margins (about 2.5cm) using 11 pts. Calibri font. You must submit your assignment as a PDF file named **CYBR373-tut2-studentID.pdf**

The criteria for grading are:

- **Completeness** – Did you complete all the tasks and how comprehensively? Did you Provide explanation where necessary?
- **Accuracy** - How well did you complete the tasks?
- **Presentation** - Did you use the right terminology? Please check for readability.

Letter grades

- **A-range:** Complete, accurate, and well presented. Shows good knowledge and good understanding of subject. Well-argued. Where required, contains good original input from the student.
- **B-range:** Mostly complete, mostly accurate, and well presented. Shows a good knowledge and good understanding of the subject but either fails to complete some parts of the tasks or is unclear or is poorly argued.
- **C-range:** Satisfactory performance although some errors in accuracy and/or problems with presentation. Shows only some basic knowledge of the subject or fails to understand some important parts of it, or does not provide solutions to a significant portion of the tasks.
- **D-range:** Poor performance overall, some evidence of learning but very problematic in all aspects mentioned above.
- **E-range:** Well below the required standard.