**COMP718 InfoSec Policy Tutorial**

**TASK A**

Refer to Table 4-1,.p.179 in the course textbook and answer the questions below in relation to AUT’s Privacy Policy ( <https://www.aut.ac.nz/__data/assets/pdf_file/0008/143279/Privacy-Policy.pdf> )

|  |  |
| --- | --- |
| **Question** | Answer |
| 1. **Is AUT’s privacy policy an EISP policy?** Explain why this policy can be considered as an example of an EISP policy**.** | Yes, AUT's privacy policy may be used as an example of an Enterprise Information Security Policy. An EISP often defines the strategic direction, scope, and tone for all security initiatives inside the firm. AUT's privacy policy establishes a strategic framework for securely processing personal information, ensuring compliance with relevant privacy legislation, and establishing privacy-related duties and responsibilities, all of which are critical components of an EISP. |
| 1. **identify three ELEMENTS of the AUT’s Privacy Policy.** Describe them, in your own words. *Note*: **.** For examples of elements, check Table 4-2. | **Purpose**: The objective section clearly outlines the policy's aim, which is to provide standards and processes for how the institution will handle personal information, ensure access to personal information, and fulfill necessary reporting needs.  **Legal Compliance**: This section describes the university's commitment to follow certain laws and regulations such as the Privacy Act 2020 and the Official Information Act 1982, ensuring that all operations are legally sound.  **Roles and Responsibilities**: This section outlines who oversees ensuring compliance with the privacy policy. It appoints Privacy Officers for various groups (workers and students) and explains their responsibilities for addressing privacy problems and compliance. |
| 1. **Are there any elements that are not** listed in Table 4-2? | ***Protection of Information:***  **Description:** This element in AUT’s Privacy Policy is primarily concerned with the measures and protocols in place to safeguard personal information from unauthorized access, use, disclosure, or destruction. The policy outlines that personal information must be handled in compliance with the Privacy Act 2020, ensuring that data is protected according to legal standards. This includes appointing Privacy Officers who are responsible for overseeing the compliance of these protective measures within the university.  ***Use of Information:***  **Description:** This element deals with the stipulations set forth regarding how personal information can be utilized within the university. AUT’s Privacy Policy specifies that the use of personal information must align with the purposes for which it was collected, as outlined in the policy, and must comply with the Privacy Act 2020. This ensures that personal information is not misused and is only used for legitimate university functions, such as academic and administrative purposes.  ***Information Handling, Access, and Usage:***  **Description:** This element focuses on the procedures and guidelines for accessing and using personal information within the university. AUT’s Privacy Policy clearly states that access to personal information is regulated and that such information can only be accessed by authorized individuals in accordance with the principles of the Privacy Act 2020. It also mentions that all requests for access under the Official Information Act 1982 are treated as requests made pursuant to the Privacy Act 2020, ensuring proper handling and access protocols are followed. |
| 1. **NEED : Is it made clear why the policy is needed?** E*xplain in your own words***.** *Hint: Find out what Privacy Principle 6 section 1b is about* | Yes, the policy is clearly needed. It is necessary to guarantee that the institution manages personal information responsibly and in accordance with the Privacy Act 2020. This is critical not just for preserving people' privacy, but also for satisfying legal requirements and sustaining the confidence of students, faculty, and others. Section 1b of Privacy Principle 6 is anticipated to address individuals' rights to access their personal information, highlighting the significance of openness and responsibility in the processing of personal data. |
| 1. **Are ROLES AND RESPONSIBILITIES outlined in this policy?** Explain**.** | Yes, the roles and duties are well defined. According to the policy, Privacy Officers are designated for staff and students, with responsibilities that include maintaining compliance with privacy principles and processing requests for access to personal information. This distinction helps to ensure that there are specific persons who are responsible for privacy issues. |
| 1. **Are REFERENCES provided?** Explain | The policy mentions relevant legislation such as the Privacy Act 2020 and the Official Information Act 1982, which are critical references for the legal framework governing the policy. Additionally, it refers to related procedures and documents that can be found on AUTi, providing a pathway for those seeking more detailed procedural information. This inclusion of references supports the policy’s credibility and utility by guiding users to additional resources for compliance and implementation. |

**TASK B**

A student has asked their lecturer at AUT to provide them (the student) with their personal information as recorded in the student record system (Arion). The student thinks that their permanent address was wrongly recorded, and they want to verify that and, if needed, the student will request to have their permanent address corrected. The lecturer is familiar with AUT’s personal information procedures (these can be found at <https://www.aut.ac.nz/privacy/privacy-policy>).

*Questions:*  should the lecturer show the student their personal information as recorded in ARION? Are there any conditions or circumstances to consider around this? Should the lecturer change the permanent address? *Provide advice to the lecturer on these three questions, from your position as an InfoSec consultant, and explain the rationale behind your advice.*

As an InfoSec consultant, here is the advice for the lecturer regarding the student's request to access and potentially correct their personal information in the ARION system at AUT:

***Should the lecturer show the student their personal information as recorded in ARION?***

**Advice:** No, the lecturer should not directly show the student their personal information.

**Rationale:** According to AUT’s privacy policy, specific roles and responsibilities are designated for handling personal information requests. Privacy Officers are appointed to manage such requests to ensure compliance with the Privacy Act 2020. Lecturers are typically not authorized to directly access or disclose personal information without following the proper protocol. This ensures the security and confidentiality of student data.

***Are there any conditions or circumstances to consider around this?***

**Advice:** Yes, there are specific procedures and legal considerations to follow.

**Rationale:** The student’s request to access their personal information falls under the Privacy Act 2020, which allows individuals the right to access their personal information. However, this request must be handled by the designated Privacy Officers or through the official channels as outlined in the privacy policy. This ensures that all requests are logged, verified, and handled consistently and that any disclosures are legally compliant

***Should the lecturer change the permanent address?***

**Advice:** No, the lecturer should not change the student’s permanent address.

**Rationale:** Modification of personal information should only be performed by individuals who have the authority and access rights to do so, typically through a formal request process. This process usually involves verifying the accuracy of the change request (e.g., by checking supporting documents) before any changes are made to ensure data integrity and compliance with data protection regulations.

***Additional Advice to the Lecturer:***

**Direct the Student to the Appropriate Procedure:** Inform the student about the proper channels for such requests, which would typically involve contacting the university’s Privacy Officer or directing the student to the student services where they can formally request to access or correct their personal information.

**Educate on Privacy Policy:** It might also be helpful to briefly explain to the student the reasons for these protocols — mainly to protect the privacy and security of student data and to ensure compliance with relevant laws.

**Documentation:** If involved in any part of the process, keep records of the interactions and communications regarding the student’s request for auditing and compliance purposes.

*By following these guidelines, the lecturer will help maintain the integrity and confidentiality of student data and ensure that the university remains compliant with applicable privacy laws and regulations.*

**TASK C**

Consider the Data Governance Policy of the University of Auckland (found at <https://www.auckland.ac.nz/en/about-us/about-the-university/policy-hub/enabling-environment/digital/data-governance-analytics/data-governance-policy.html> ) and answer the questions below.

|  |  |
| --- | --- |
| **Question** | **Answer** |
| 1. **Is this policy an ISSP policy>** Explain why this policy can be considered as an example of an ISSP policy | **Yes**, this policy is an example of an Issue-Specific Security Policy (ISSP). ISSPs focus on certain areas of technology that require management's attention and specific advice. This Data Governance Policy focuses on the administration, preservation, and use of institutional data inside the University. It defines roles, data quality standards, and access restrictions, all of which are common features of an ISSP that focuses on a specific issue inside an organization's broader security architecture. |
| 1. **Identify any three ELEMENTS in this policy.** Describe them in your own words. *Note*: For examples of elements, check Table 4-3; however, you may find that the policy has element(s) that are not listed in Table 4-3. | 1. **Data Governance:** This element outlines the overarching framework and principles for managing institutional data as a valuable asset of the University. It emphasizes that no single person or department owns the data, but specific units are responsible for developing data management plans that ensure data quality, availability, and accessibility. This ensures a structured approach to handling data across the university. 2. **Data Quality:** This section of the policy focuses on maintaining high standards for the data held by the University. It includes avoiding unnecessary duplication, defining and monitoring quality standards, and managing institutional metadata. The aim is to ensure that the data is complete, valid, consistent, timely, and accurate for its intended use, which is crucial for the reliability of the University's operations and decision-making processes. 3. **Data Access:** This element addresses the protection of data from unlawful or unauthorized access, use, or disclosure. It also includes the development of contingency plans to handle emergencies that could affect systems containing institutional data. Additionally, it specifies the conditions under which different levels of aggregated data are accessible within the University, promoting transparency while safeguarding sensitive information. |