Office of the Victorian Information Commissioner

PRIVACY

Examination of Victorian universities' privacy and security policies

Examination under section 8C(2)(b) of the *Privacy and Data Protection Act 2014* (Vic)

OVIC

Authorised by the Victorian Information Commissioner

Published by the Office of the Victorian Information Commissioner
PO Box 24274
Melbourne, Victoria, 3001

t: 1300 006 842
e: enquiries@ovic.vic.gov.au
w: ovic.vic.gov.au

Disclaimer
This publication may be of assistance to you, but the Office of the Victorian Information Commissioner and its employees do not guarantee that the publication is without flaw of any kind or is wholly appropriate for your particular purposes and therefore disclaims all liability for any error, loss or other consequence that may arise from you relying on any information in this publication.

Date of publication
June 2021

Table of contents

Foreword

The protection of information by universities has come under focus in recent years as a number of Australian universities have been subject to cyber security attacks. These attacks highlight the risks posed by data breaches and the potential impact on thousands of students, staff and research participants. That led the Privacy and Data Protection Deputy Commissioner to conduct this examination into the policies and procedures that Victorian universities have implemented to protect the personal information that they hold from loss and misuse.

The report shows that Victorian universities have in place a wide range of policies and procedures to identify and secure the personal information they hold. There are, however, areas for improvement identified in this report and I encourage universities to consider these as they review and update their personal information policies.

Victorian public sector organisations can take a variety of steps to protect personal information from loss or misuse, and for this reason comparing the results of one university against another should be approached with caution. The examination was undertaken with a view to examining the completeness of universities' policy frameworks, not with a view to creating a leader board of progress.

The report shows that Victorian universities are taking cyber security seriously. Most Victorian universities are taking steps, such as internal and external audits and assessments, to obtain an accurate picture of their capability and threat landscape with respect to information security. However, more work needs to be done in several areas.

Thank you to the universities for providing responses to our request for documentation. OVIC appreciated receiving detailed and thorough responses from most of the universities participating in the examination. My office looks forward to continued engagement with them.

Sven Bluemmel
Information Commissioner

29 June 2021

Executive summary

OVIC conducted the examination to inform itself and the public about how universities protect personal information. OVIC found that all Victorian universities:

- have a data breach response plan that includes the steps contain, assess, notify and review
- conduct Privacy Impact Assessments (**PIAs**) for new projects involving personal information. Several universities reported that they are working to embed PIAs into security and procurement processes to promote a high completion rate
- conduct privacy and data security online training for staff
- have prioritised ICT and cyber security risks.

We observed that:

- universities were less focussed on managing risks to personal information involving physical and personnel security
- many universities do not have clear policies and procedures to guide staff to destroy personal information when it is no longer needed
- most universities do not have written guidance about sharing personal information with third parties.

OVIC makes several recommendations for universities, detailed below. The areas that require attention are policies and procedures for:

- considering the nature of personal information and applying protective markings to communicate the nature of information
- destroying personal information when it is no longer needed
- considering notifying OVIC of a data breach
- sharing personal information with third parties and engaging contracted service providers that handle personal information on their behalf
- privacy and information security training to all personnel with access to personal information, including contractors.

Introduction

Background

1. The Victorian public university sector comprises eight universities. The primary role of the universities is to provide higher education and conduct research. In the course of educating and researching, universities collect and handle a vast amount of personal information about individuals, from information about students, staff, or research participants. In 2019 there were over 300,000 students enrolled in Victorian universities.[1]

2. In Victoria, most universities are required to comply with Part 3 of the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**), which provides for the responsible handling of personal information by public sector organisations.

3. The eight universities in Victoria subject to Part 3 of the PDP Act[2] are:

   - The University of Melbourne (**UoM**)
   - Monash University (**Monash**)
   - La Trobe University (**LTU**)
   - Deakin University (**Deakin**)
   - Victoria University (**VU**)
   - RMIT University (**RMIT**)
   - Swinburne University of Technology (**Swinburne**)
   - Federation University of Australia (**Federation**)

4. This report outlines the findings from an examination of these universities' privacy and information security policies. OVIC conducted a survey of the universities to collect relevant policy and procedure documents, and assessed these against IPP 4, which requires public sector organisations to take reasonable steps to protect the personal information they hold.

The requirement to secure personal information under IPP 4

5. Personal information is defined in section 3 of the PDP Act, when an organisation captures information about an individual who is identified or whose identity is reasonably ascertainable.

6. Where a Victorian university collects, holds, uses or discloses personal information, it must comply with the 10 Information Privacy Principles (**IPPs**) listed in Schedule 1 of the PDP Act. The IPPs set out the minimum standard for how the Victorian public sector should handle personal information, from the time it is first collected until it is disposed of when no longer required.

7. IPP 4 contains two distinct obligations:

   IPP 4.1 – An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

[1] VAGO (Victorian Auditor-General's Office) (2019) Results of 2019 Audits: Universities, State Government of Victoria, accessed on 14 April 2021.
[2] The listed universities fall within the scope of Part 3 of the PDP Act because they are captured by the definition of 'university' in section 1.1.3 of the *Education and Training Reform Act 2006* (Vic).

IPP 4.2 – An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.

8. IPP 4.1 is underpinned by a risk-based approach to protecting personal information. Risk-based means taking reasonable and proportionate steps in response to identified data security risks. Security risks can exist across different areas, such as governance, information, personnel, ICT, and physical security.

OVIC's examination

Reasons for examining Victorian universities

9. OVIC chose to examine the data security practices of universities because:

   a. Universities hold the personal information of many thousands of Victorians, including sensitive personal information and other types of personal information that could harm individuals if misused or in the event of a data breach.

   b. 'The protection of personal information in the Victorian higher education sector' is one of OVIC's regulatory priorities for 2020-2021.

   c. A number of high-profile security breaches at Australian universities have occurred in recent years, and the threat of cyber security attacks against the higher education sector is thought to be increasing.[3]

   d. The Victorian Protective Data Security Framework (**VPDSF**) and accompanying Victorian Protective Data Security Standards (**the Standards**), issued under Part 4 of the PDP Act provide direction to Victorian public sector organisations on their data security obligations. Under the VPDSF organisations are required to submit a Protective Data Security Plan to assist them to develop better security, and to advise OVIC of the implementation status of the Standards and their organisation's maturity level. The VPDSF does not generally apply to Victorian universities, so OVIC does not receive regular reporting about the status of universities' security maturity as it does for other VPS organisations that are covered by Part 4 (Data Protection) of the PDP Act.[4]

   e. Universities are complex organisations with many different but interlinked business areas, involving teaching, research and other functions. It can be challenging for a university to implement effective data governance, especially where the business units operate separately (for example, where they use different technology and systems).

[3] An article in *iTnews* on 11 March 2021 reported on the views of security staff at the Australian Security Intelligence Organisation and the Department of Home Affairs about the significant and increasing threat of cyber security attacks against the higher education sector in Australia. Ry Crozier (11 March 2021) 'ASIO's Mike Burgess says he knows who attacked ANU', *iTnews,* accessed on 15 April 2021.

[4] While section 84(2)(a) of the PDP Act excludes Victorian universities from the application of Part 4 of the Act, there are some situations where a university also delivers the functions of a TAFE. As TAFE institutions are public entities, Part 4 of the PDP Act may apply to parts of these universities' activities. There are currently four dual-sector universities within Victoria: RMIT University, Swinburne University of Technology, Victoria University, and Federation University.

Scope of the examination

10. OVIC examined Victorian universities':

    a. privacy and information security policies and procedures

    b. methods of identifying and recording holdings of personal information

    c. approaches to assessing the security value or nature of personal information

    d. approaches to risk management with respect to personal information security risks.

11. In this examination, OVIC reviewed the universities' risk assessment policies but did not review any risk assessment outcomes or evaluate the security controls adopted by universities for any particular data sets. Further, it was outside the scope of this examination to verify whether a university adhered to its own policy or procedure.

How the examination was conducted

12. In October 2020, the Privacy and Data Protection Deputy Commissioner wrote to the Vice Chancellors of the Victorian universities to commence the examination and request information.

13. The information reviewed as part of the examination was either provided by the universities in response to OVIC's request or was available through the universities' websites.

14. OVIC developed and applied a framework to assess the information and policy documents regarding their support for compliance with IPP 4.

Examination report

15. As well as exploring the findings of the examination, this report contains lessons for improving the protection of personal information through policies and procedures.

16. The lessons contained in this report are relevant to all Victorian public sector organisations and will be particularly useful for organisations that engage or employ a large number of personnel or hold personal information across different business areas.

What we found – summary

17. The charts in this section show whether each university has a documented policy, procedure or mechanism to support compliance with IPP 4 in the following areas:

    - Identifying and documenting personal information holdings
    - Identifying the value or sensitivity of personal information holdings
    - Identifying security risks to personal information security
    - Managing and implementing measures to address risks
    - Destroying or permanently de-identifying personal information
    - Sharing personal information with third parties
    - Engaging contracted service providers for services that involve handling personal information on behalf of the university
    - Responding to data breaches
    - Delivering privacy and information security training

18. OVIC acknowledges that the universities surveyed have different levels of resourcing, scales of operation, and governance arrangements. The features of each university will impact on the risks to personal information security, as well as the resources and capability available to address those risks.

19. Where a university has not achieved a 'yes' rating this does not mean OVIC is of the view that the university has failed to comply with IPP 4. Rather, OVIC has identified an area of risk that a university should assess whether it has taken 'reasonable steps' to address. Universities may be protecting personal information in other ways than through the sort of policies and procedures that OVIC examined.

20. In response to OVIC's assessment of each universities' policy and procedure documents, many universities advised that they are developing additional resources to address gaps identified by OVIC's assessment or as part of a universities' auditing processes.

21. The following key is applicable to the charts in this report and the table below:

    Yes – The university has a documented policy, procedure or mechanism that addresses OVIC's question.

    No – The university has not demonstrated that it has a policy, procedure or mechanism that addresses OVIC's question.

    Partial – The university:

    a. has a documented policy, procedure or mechanism that partially addresses OVIC's question; or

    b. has described a policy, procedure or mechanism that addresses OVIC's question, but this is not documented; or

    c. the university was taking steps to address OVIC's question (e.g., a relevant policy was under development) at the time the examination commenced.

	Did the university have a policy, procedure, or mechanism for:									
	Identifying and documenting its personal information holdings?	Identifying the value or sensitivity of its personal information holdings?	Identifying security risks to personal information?	Managing and implementing measures to address risks?	Addressing when and how personal information holdings should be destroyed or permanently de-identified?	Responding to a data breach with the key steps of contain, assess, notify, and review?	Considering personal information security risks when considering whether to engage a contracted service provider?	Implementing contractual mechanisms to ensure personal information is protected?	Determining when and how it is appropriate to share personal information with third parties?	Conducting personnel training on privacy and information security?
UoM	Partial	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Partial	Yes
LTU[5]	Yes	Partial	Partial	Partial	Partial	Yes	Partial	Yes	Partial	Yes
Deakin	Partial	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Federation	Partial	Yes	Partial	Partial	No	Yes	No	Yes	Yes	Yes
RMIT	Yes	Yes	Yes	Partial	Partial	Yes	Yes	Partial	No	Yes
Monash	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Swinburne	No	Partial	No	Yes	Yes	Yes	No	Yes	Partial	Yes
VU	Partial	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

[5] During the examination, La Trobe University only provided OVIC with publicly available policies and procedures to assess. It may have achieved a higher rating had OVIC been provided with internal policies and procedures.

What we found – in detail

PART 1 – Approaches to identifying personal information held across an organisation

22. OVIC examined how privacy staff at each of the Victorian universities maintain awareness of the personal information their university holds. Universities are typically large organisations that consist of distinct areas (such as faculties, institutes and business areas) carrying out various operations.

23. OVIC asked the universities whether they maintain a central record of their personal information holdings, to support their management and protection of this information.

Why should organisations maintain oversight of the personal information they hold?

24. Privacy officers and data governance teams of Victorian public sector organisations should maintain oversight of the amount and categories of personal information held by their organisation. The information may be stored in various locations such as in physical records and within electronic business systems.

25. Oversight enables privacy officers and data governance teams to provide informed advice to business units about the steps that should be taken to protect personal information. It also supports the development and implementation of effective policies and procedures. For example, an ICT security policy can be developed that appropriately reflects the sensitivity of information held in those ICT systems.

Information Asset Registers

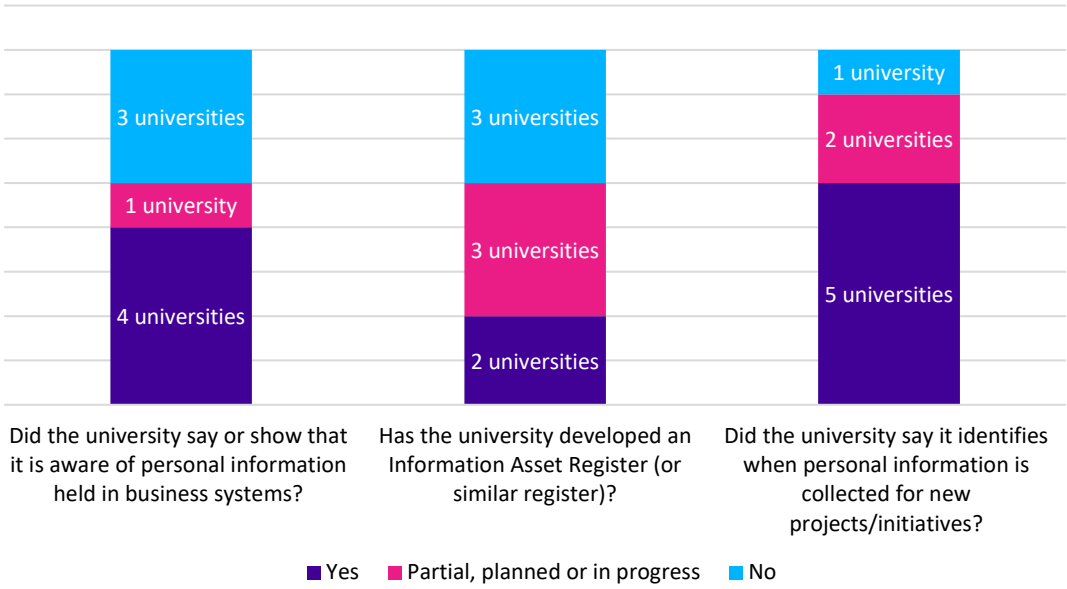
26. An Information Asset Register (**IAR**) is a register that records an organisation's information holdings or assets. Information assets are bodies of information that have value to an organisation, and do not just include personal information. Organisations can flag assets in an IAR that contain personal information.

27. An IAR allows organisations to maintain an understanding of types of personal information they hold, and where it is held (in both physical and electronic locations).

28. Organisations do not need to develop an IAR to comply with IPP 4.1. However, IARs are a useful tool that supports the protection of personal information by assisting organisations catalogue the personal information they hold.

Examination findings

Chart 1 – Illustration of methods described by universities for identifying personal information holdings



Do universities identify the personal information they hold?

29. OVIC found that:

    a. **Two** universities currently record holdings of personal information in an Information Asset Register (**IAR**) (or similar centralised register).

    b. **Three** universities plan to develop an IAR this year or are currently developing an IAR.

    c. **Three** universities do not have and do not plan to develop an IAR.

30. **Four** universities said that although they did not have an IAR, they maintained awareness of their personal information holdings in key business systems, such as through completing a Privacy Impact Assessment (**PIA**) for these systems or through completing architecture maps.

31. **One** university explained that it undertakes Record Assessments to accurately identify information to record in its IAR. The assessments are performed on business systems to identify datasets that contain personal and/or sensitive information, which can then be incorporated into the university's IAR.

Other methods of identifying where and when personal information is collected and held

32. **Five** universities completed a PIA or other risk assessment for new projects that enable those universities to identify when personal information may be collected and held.

Observations

33. It is not compulsory for Victorian universities to develop an IAR to ensure it implements reasonable steps to protect the personal information it holds, as required by IPP 4.1.[6] However, it is important that Victorian universities and other organisations subject to IPP 4.1 have a comprehensive understanding of the personal information they hold. This is because it is difficult for any organisation to protect information that it does not know it holds.

34. The benefits for organisations that develop a centrally held recording of personal information holdings (such as in an IAR) include:

    a. central oversight

    b. an accessible and easy to refer to resource for ongoing risk assessment.

35. Organisations may place the responsibility to identify and manage personal information on its business units, rather than employing a central strategy to manage and protect personal information at an enterprise level. For this strategy to be effective, thorough policies, procedures and training will likely be needed. It is also important that staff know who to contact for privacy and information security advice. In a decentralised model, staff responsible for projects that span multiple locations, business units or faculties (for e.g., a project to implement a new ICT system), may find it more difficult to identify and manage personal information security risks.

36. PIAs and Information Security Risk Assessments (**ISRAs**) can support the identification of personal information holdings. Organisations that rely on PIAs as their primary method may only be identifying their holdings of recently collected personal information, as they are most likely completed in response to a new project. This may leave privacy teams and wider staff, unaware of the historical or legacy information held by the organisation. The effectiveness of PIAs and risk assessments in informing an organisation about the personal information it holds depends on how long it has been carrying out PIAs and if there is another strategy in place to identify personal information held in existing systems, such as by completing Record Assessments.

[6] VPS organisations that are covered by Part 4 of PDP Act are required to report on their implementation of the Victoria Protective Data Security Standards (**VPDSS**). Element 2.020 of Standard 2 of the VPDSS is 'The organisation identifies, documents, and maintains its information assets in an information asset register (IAR) in consultation with its stakeholders.'

PART 2 – Identifying the security value, or assessing the sensitivity of, personal information

Identifying the sensitivity of personal information

37. Assessing the nature of personal information involves determining if the personal information is sensitive information, as defined in Schedule 1 of the PDP Act, or if the disclosure of the information, because of its nature, may cause a higher degree of harm to an individual. This is an important part of understanding the value of the personal information. For example:

    a. sensitive information such as a person's racial or ethnic origin can be used to discriminate, or

    b. financial information can be used in identity fraud or to cause financial harm.

38. By being aware of the value of personal information, organisations are best placed to take 'reasonable steps' to protect it. How sensitive personal information may be generally aligns to the level of harm to an individual that may be caused if the information was compromised. The level of security applied to records of personal information or data sets containing personal information should reflect the sensitivity of the information.

Identifying the value of public sector information

39. Identifying the value of information is a security practice that applies to all information an organisation holds (including but not limited to personal information). Through assessing the security value of information, organisations can identify and apply appropriate measures to secure information that are proportional to the harm that could occur if the information were compromised.

40. For Victorian public sector organisations, assessing the security value of information involves determining the impacts to government operations, organisations or individuals, if there were a compromise of the confidentiality, integrity and/or availability of public sector information.

41. Like the concept of assessing the sensitivity of personal information, assessing the security value of public sector information can assist VPS organisations to implement appropriate security measures in consideration of the potential harm to the individual if their information was lost or misused.

Examination findings

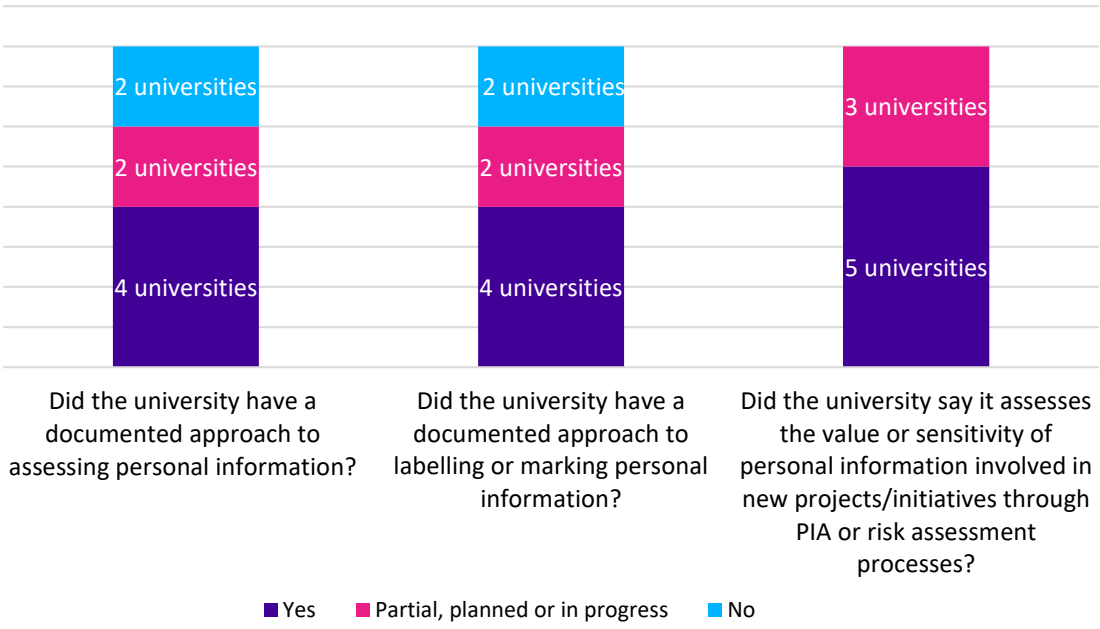
Do Victorian universities assess the sensitivity or the value of the personal information they hold?

42. **Four** universities showed they have information management and classification frameworks. These documents generally set out how the universities assess the security value of information.

43. Of the four, **two** universities' processes for assessing information specifically required the user to consider if the information assets or data sets contained personal information.

How do Victorian universities assess the sensitivity or the value of the personal information they hold?

Chart 2 - Methods described by universities for assessing personal information



Approaches to assessing personal information

44. Column 1 in the table above includes responses rated 'partial'. In one case, a university explained that it is developing a Data Governance Policy and Framework. Another university has a process for undertaking PIAs that involves assessing the personal information in accordance with the university's Information Security Policy, which contains data classifications. This response was rated 'partial' to reflect that the university did not have a documented approach for assessing personal information that applies more broadly outside of the PIA process.

Applying markers to information to communicate the information's value or sensitivity

45. OVIC found that following assessment, **four** of the frameworks/procedure documents required staff to apply a protective marking to information (for example, documents, emails) that governs how that information needs to be handled. For example, one university classifies data into four categories:

    a. strictly confidential

    b. restricted to staff

    c. restricted to staff and students

    d. public.

46. Of the **four** universities that had a documented approach to labelling or marking personal information, **three** universities classify information according to the impact of a compromise to the confidentiality, integrity and/or availability of information.

Assessing the nature or sensitivity of information through Privacy Impact Assessments

47. **Five** universities' responses explained that when they conduct a PIA for a new project or initiative, they consider the nature of the personal information involved.

48. **Of the five, two** universities said they assessed the value of personal information through PIA processes but did not have a separate process to assess security value.

Observations

49. Where the PIA process may be effective in valuing newly collected personal information, its application is restricted where it is not used to assess the value or sensitivity of existing personal information held by the university.

50. Having a documented approach to assessing the value of information supports staff to identify its value consistently and apply reasonable measures to protect the information**.**

Recommendations

51. OVIC recommends universities consider developing, where they have not already done so:

    a. policies to support staff to consider the nature of personal information to support organisations in ensuring they apply appropriate protections to personal information.

    b. a mechanism to apply protective markings to information (for e.g., emails or documents) in a way that consistently communicates the security value or nature of the information.

PART 3 – Identifying and managing security risks to personal information

52. As explained earlier in this report, organisations should consider data security risks, and take reasonable steps (i.e. implement controls) to address those risks across:

    a. governance

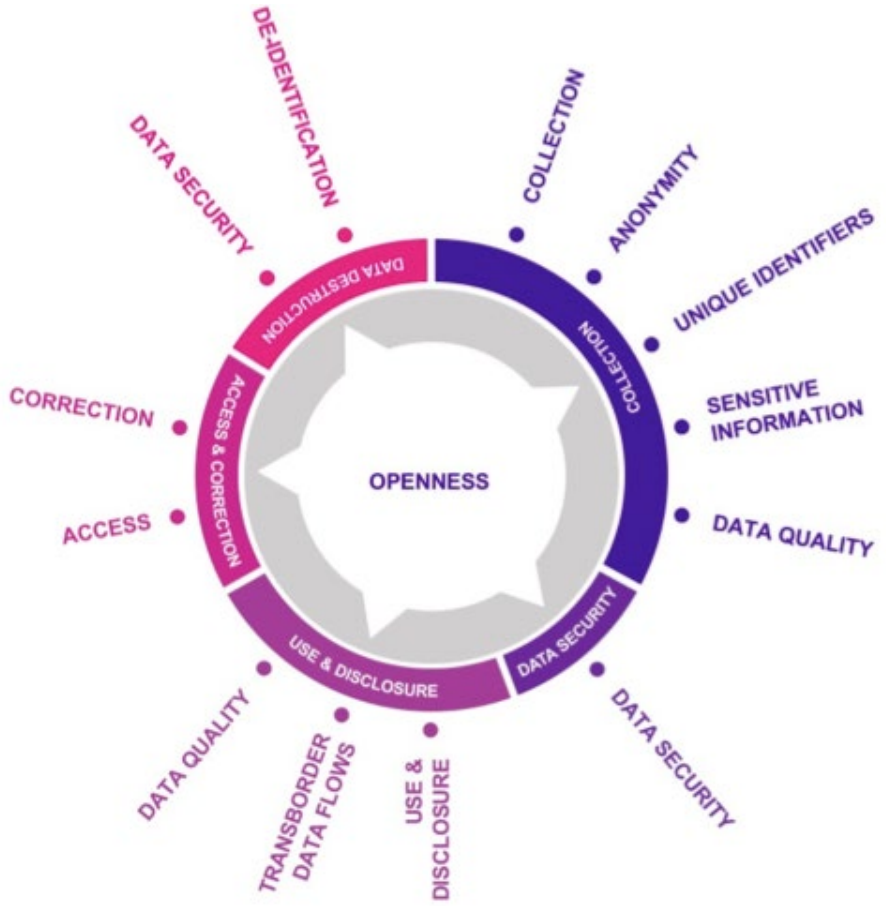
    b. information security

    c. personnel security

    d. ICT security

    e. physical security.

53. In addition, organisations should be aware that risks in information security can change throughout the information lifecycle. The diagram below illustrates how the IPPs fit into the lifecycle of information, beginning with collection.



54. Having a comprehensive process or policy in place that sets out how an organisation identifies and manages information security risks assists the organisation to protect personal information consistently and ensure it considers all the risk areas.

Examination findings

55. OVIC asked the universities to describe how they assess security risks to their personal information holdings and their process for identifying appropriate security measures to apply in response to identified risks.

56. OVIC found that:

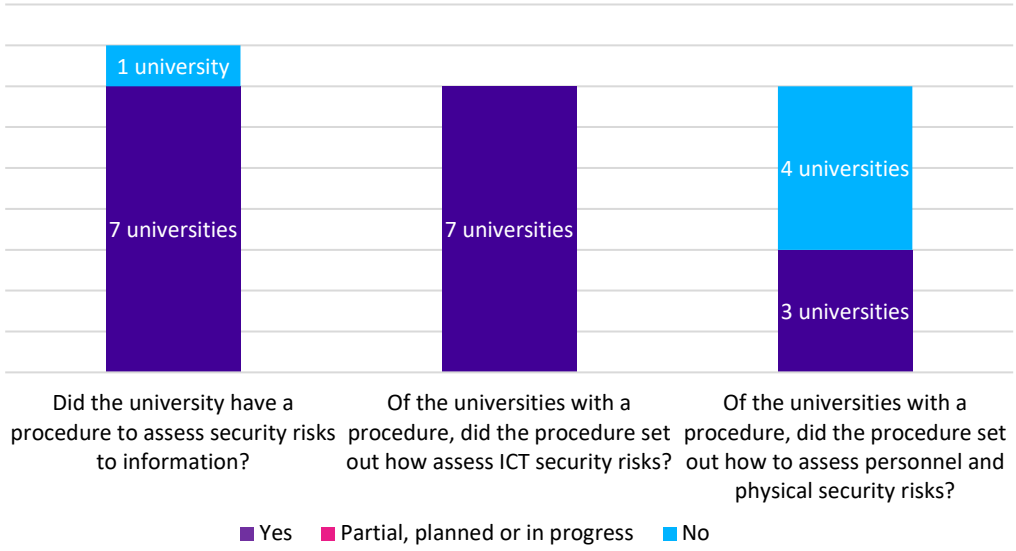
    a. **Six** universities had enterprise level Risk Management Frameworks or processes. These kinds of documents were overarching and do not refer to specific kinds of risks. The documents often included a Risk Matrix to rate risks by considering different impacts.

    b. **Two** universities had ICT security policies that sets out a framework for management of risks with respect to ICT based personal information.

    c. **Four** universities explained that they performed risk assessments for new projects (mostly IT related projects).

57. OVIC found that the universities generally displayed a stronger focus on identifying cyber and ICT information security risks above the consideration of risks for the other security domains.

Chart 3 – Approaches to identifying security risks to personal information



58. Column 2 and 3 of the above chart only has 7 universities in total, because it includes only the universities that received a 'yes' rating from OVIC in response to the question 'Did the university have a procedure to assess security risks to information?'

59. OVIC found that the staff responsible for identifying and applying security measures to protect information at universities most often belonged to IT/cyber/'eSolutions' teams. **One** university had established a specific unit that is responsible for managing hard copy information security risks.

60. Some universities' descriptions of security measures applied to protect personal information included the following activities:

a. cyber due diligence for service providers

b. complete a checklist for security measures for IT procurement.

61. In the universities' responses to OVIC asking how they identify security controls to protect personal information, most of the universities did not explain how they consider and select personnel and physical security controls. This means that the examination could not verify that Victorian universities are generally considering security controls across all of the security areas (governance, information, personnel, ICT and physical).

62. Overall, the universities did not present to OVIC a holistic approach to securing personal information as they displayed a heavy focus on ICT/cyber as the key driver of risk. This means that they may not be considering other important risks factors, such as personnel and physical security.

Did the universities have procedures for protecting high risk and sensitive personal information?

63. Universities' approaches to protecting high risk and sensitive personal information mostly focused on identifying this information and applying a data classification or label, or marking this information in a university's IAR.

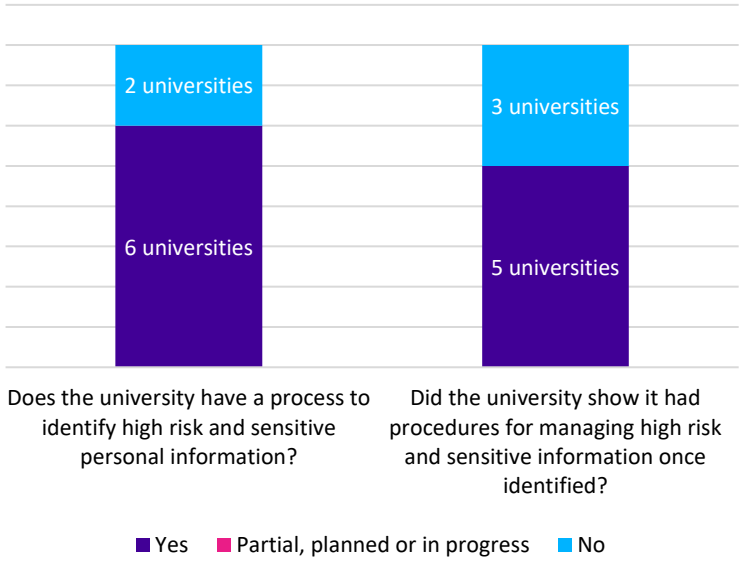
64. Some universities provided details about procedures for handling high risk or sensitive information that covered specific circumstances (for e.g., handling of sensitive HR records). These circumstances included:

a. Specific training for staff, depending on the information they handle in their role.

b. Classification frameworks to provide direction to staff on handling information in accordance with the information's classification.

c. One university provided a checklist for engaging contractors that required 'background checks of its staff commensurate with their level of access to systems and data they may have and maintain security clearances where required for staff with access to highly sensitive data.'

Chart 4 – Approaches to protecting high risk and sensitive personal information



Observations

65. The universities generally showed a strong focus on cyber security, which may be prioritised above other security areas such as personnel and physical security.

66. OVIC considers that it is best practice for high level frameworks to be integrated with specific procedures to address risks to personal information across governance, information, personnel, ICT, and physical security.

67. As risks change (for e.g., when an organisations information handling practices change) organisations need to ensure that risk assessments are reviewed frequently to enable staff to identify new risks. Risks should be managed through the universities' existing risk management framework, with risks being reviewed at regular intervals or whenever an incident occurs, whichever is sooner.

68. Identifying sensitive and high-risk information is a significant part of the work needed, but it is also critical for organisations to have appropriate policies and procedures to manage the protection of information, and for staff to be appropriately trained and aware of organisation expectations.

PART 4 – Policies and procedures that support compliance with IPP 4

69. Thorough and appropriate policies and procedures support the protection of personal information. Documentation (such as policies, procedures, standards, quick reference guides) can communicate to personnel how the organisation expects information to be handled. Policies and procedures can prevent the improper handling or disclosure of personal information in various circumstances.

70. In addition to the documentation examined in the preceding sections of this report, OVIC examined documentation covering the following areas:

    a. Destruction and permanent de-identification of personal information

    b. Data breach response

    c. Engaging contracted service providers (**CSPs**) and other third parties that may receive or hold personal information on behalf of a university

    d. Training for university personnel about privacy and data protection

Examination findings

Prevalence of policies and procedures that support data security

71. The table below represents the prevalence of different policies and procedures that support data security.

Document	Purpose of document	Prevalence	Observations
Privacy policy/ procedure	Contains statements about how an organisation manages personal information, as required by IPP 5. Organisations should demonstrate in a privacy policy, procedure or collection statement how the organisation securely stores personal information.	**All** available online	**Review schedules for privacy policies/procedures** • **Five** universities update their privacy policies every 2-3 years. • **Two** universities update their privacy policies every 5 years. • **One** university was updating their privacy guidelines in Nov 2020 after it was introduced in 2014. **Security excerpts** • **Most** policies stated that the university will take reasonable steps to protect personal information from misuse, loss, unauthorised access, modification or disclosure. • **Some** universities referred readers to processes (e.g.,
Privacy/Collection statement		**All** universities said they have various collection statements, for example, for staff, students, public.	

			Information Security Policy) that set out security requirements. • **One** policy outlined some of the physical and electronic safeguards in place to protect personal information.
Data breach response plans	A data breach response plan assists organisations to respond to the privacy implications of a data breach and minimise the harm to affected individuals.	**All** had a relevant policy that assisted staff to respond to a data breach.	
General critical incident response policy/procedure	Critical incident response documents may set out an organisation's approach to responding to a number of incidents, including data breaches or refer users to the organisation's data breach response plan.	**All** had incident management or business resilience policies or systems.	
Information security policy	Sets out how an organisation maintains the security of their information, for example by setting out requirements for personnel to adhere to.	**Five** universities have an Information Security Policy. **Three** have an Electronic Information Security Policy or ICT/IT Security Policy.	With regard to the three universities' focus on electronic information policies, it is not known if the universities have a separate document that sets out how hard copy information is secured.
Information security procedures	Procedures may set out how information security is maintained in specific circumstances, for example, when personnel use university devices.	**All** universities provided information about/copies of various information security procedures.	Information security procedures included: • Acceptable use standard • User device standard • Information classification procedures • Management of Special Category Information Instruction
Risk management policies	Sets out the organisations approach to risk management, for example, by setting Risk Appetite Statements (tolerance levels for risk). The approach may cover data security risks.	**All**	Risk management policies are generally reviewed more regularly by the universities. At least **three** universities' policies have a one-year review period.

Records management policy/procedure	Assists organisations to manage information in consideration of the information lifecycle and destroy information when it is no longer needed.	**All**	**Three** universities were reviewing their records management documents as at November 2020.

Did the universities have up to date policies and procedures?

72. Overall, OVIC found 73% of all policies and procedures across all the universities were current, having been produced in the last 1-5 years, and reviewed in line with the universities' review schedule. The remaining 27% were either not currently in place, were under review, or OVIC could not establish review dates or timeframes.

Staff accountability for policies and procedures

73. OVIC found that key accountabilities for the universities' policies and procedures were generally set out in the document. For example, the obligation to require staff to comply with a policy, to update a policy, to be a contact point for questions about the policy etc.

74. Some universities provided a diagram that represented the roles responsible for information security and privacy, and the reporting structure for these roles.

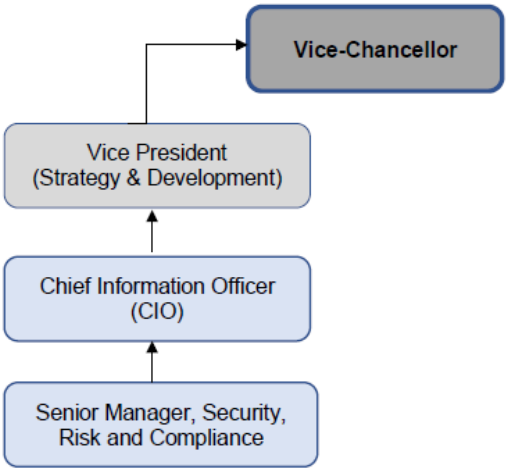
75. The table below is an example of a table taken from one universities' Privacy Policy, describing the roles and responsibilities of individuals working in privacy and data protection.

Role/Decision/Action	*Responsibility*	*Conditions and limitations*
The Privacy and Data Protection Officer must control and maintain the Privacy Policy	University Secretary	
The Privacy and Data Protection Officer must administer this policy, including monitoring compliance, informing and assisting staff on privacy issues and responding to complaints concerning potential privacy breaches	University Secretary	
The Privacy and Data Protection Officer is the contact point for the purposes of the GDPR	University Secretary	

76. Similarly, a different university provided the table below taken from their Records Management, Disposal of Records procedure policy.

Roles	Responsibilities
Manager	a. Authorising the destruction of records in their organisational area. b. Ensuring regular and systematic disposal of records in accordance with these procedures. c. Responsible for monitoring compliance with records management legislation, policies and procedures within their organisational areas.
Records and Archives Services	a. Providing advice on the disposal of records, particularly how long records should be kept. b. Ensuring retention periods in the BCS reflect legal and business requirements. c. Responsible for monitoring overall (University wide) compliance with records management legislation, policies and procedures.
University Archivist	Determining whether records should be transferred to the University Archives, based on the BCS and the PROV RDAs.

77. Alternatively, the diagram below represents an Accountability Structure for one university's Information Security policies and procedures.



Destruction and permanent de-identification of personal information

78. IPP 4.2 requires organisations to take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.

79. Victorian universities are required to comply with record-keeping obligations under the *Public Records Act 1973* (Vic). Retention and Disposal Authorities (**RDAs**) set by the Public Records Office Victoria (**PROV**), establish how long specific types of information must be retained for, and when records can be destroyed. With respect to personal information, after minimum retention periods have expired and the information is not needed for another purpose VPS organisations are required to take reasonable steps to destroy or de-identify the personal information.

80. OVIC found that **all** universities provided or had publicly available records management policies. The focus of most of records management policies or record disposal procedures was on retaining information in accordance with RDAs issued by PROV.

    a. **Three** universities' policies/procedures provide for disposal of information when there is not a requirement, such as under the university's Retention and Disposal Authority, to keep the information.[7]

    b. **One** university's policy refers specifically to personal information and states that personal information must be 'disposed of in line with the requirements of relevant legislation (including, but not limited to the Information Privacy Act, Freedom of Information Act and Public Records Act)'.

    c. **No** policies or procedures contained instructions for staff about the measures that are appropriate, and organisationally approved, where it is no longer needed.

81. **Two** of the universities policies permitted destruction of information by one area of the university to ensure that PROV requirements are adhered to. In contrast, **one** university has

[7] Since November 2020 (when this information was collected), two universities have updated their procedures to set out the requirements to dispose information in greater detail. One of the universities procedure documents now says 'Temporary records that contain personal information must be destroyed as soon as possible after their stated retention period in the RDA. This ensures that the University meets its obligations under the Data Protection and Privacy Act.'

a Records Disposal Toolkit that aimed to support staff to delete personal information where it is appropriate themselves.[8]

82. **Three** universities' privacy policies referred to destruction or permanent de-identification of personal information (rather or in addition to universities' records management policies). Where a reference to destruction or permanent de-identification was included, generally the privacy policies said that the university would not keep the information when it was not needed for any purpose.

83. Overall, where universities do not adequately identify and record the purpose of maintaining information holdings there is a risk that universities keep information for longer than is necessary. This increases the security to information that is kept for longer than necessary. Failure to identify and record the 'need' for information also poses risks of that information being used for a secondary purpose, in breach of IPP 2 (further discussion of IPP 2 at paragraph 86).

Data breach response

84. OVIC found that **all** universities have a data breach response plan that covers the following key steps:

    a. containment of a data breach and preliminary assessment

    b. evaluating the risks associated a data breach

    c. notification (internal notification and to external parties)

    d. review of the data breach to prevent future breaches

85. Several universities' policies set out the process for responding to a data breach in additional detail to OVIC's recommended key steps, such as by:

    a. Including a Privacy Breach Matrix that differentiates levels of risk (minor, moderate, major, and extreme) resulting from a data breach.

    b. Describing different kinds of potential incidents to increase staff awareness of what constitutes a data breach.

    c. Setting out the circumstances in which notification to external parties should occur, such as to OVIC and other parties, including law enforcement.

Internal reporting and escalation of data breaches

86. **One** university's response plan stated that an incident should be discussed first with the individual's manager. **Seven** universities' documents referred users to contact their university's Privacy Officer (or another staff member with privacy responsibilities) immediately or as soon as possible.

Notification to OVIC and affected individuals

87. While all data breach response procedures contained the 'notification' step, OVIC found that two documents did not specify OVIC, either referring users to consider notification to the

Office of the Australian Information Commissioner or to the 'relevant regulatory agency', without providing further information or context.

Contracted Service Providers and third parties

88. Universities may share personal information with third parties. In doing so, universities need to adhere to IPP 2. IPP 2.1 permits the use and disclosure of personal information for the primary purpose for which it was collected. Under IPP 2.1(a), an organisation can use and disclose personal information for a related secondary purpose, if the individual the information is about would reasonably expect the organisation to do so.

89. Universities may have information sharing agreements, for example, to enable them to collaborate with other researchers or educational institutions.

90. As well as considering whether IPP 2 permits disclosure of the information, universities should determine if sharing information presents information security risks that the university needs to take reasonable steps to address.

91. OVIC found that:

    a. **One** university said it had a procedure for deciding when and how it is appropriate to share personal information with third parties in the form of specific guidelines for disclosure to external agencies, such as law enforcement, in the context of student or staff welfare and safety and security matters.

    b. **Two** universities use PIAs to determine if sharing of personal information is appropriate.

92. Many universities referred to their privacy policies or collection statements that set out the circumstances in which personal information is shared. While **all** universities described in collection statements or privacy procedures how information may be disclosed, the lists of circumstances were non exhaustive.

93. **Three** universities provided information about the contractual arrangements the university generally binds a receiving party to. OVIC received:

    a. A template clause for information sharing arrangements it enters with research collaborators. This clause says that where a party provides the other with personal information, it needs to make the other party aware of legal obligations around use, storage, and disclosure of the personal information, and comply with those 'legal and contractual obligations.'

    b. A template Memorandum of Understanding used for preliminary discussions. The university explained that a formal contract is required before any work is commenced with a third party.

    c. A template course provider agreement that binds the provider to the PDP Act.

94. In addition, **four** universities said that staff need to obtain their legal teams' approval for sharing information. **Two** of the four universities showed that this requirement was set out in a policy document (such as a Contract Management Policy).

Engaging contracted service providers that handle personal information

95. Universities, like many VPS organisations, may frequently enter into outsourcing arrangements with third parties. Where these arrangements involve the contracted service provider (**CSP**) collecting or holding personal information on behalf of the VPS organisation, the default position under the PDP Act is that the outsourcing party is liable for any privacy breaches that may occur in relation to services provided under the outsourcing arrangement, even if those breaches are the result of the acts or practices of the CSP.

96. OVIC examined:

    a. Whether universities commonly bind CSPs to the IPPs under contract.

    b. Whether universities undertake any further steps to ensure personal information held by CSPs on their behalf is adequately protected.

97. **Seven** universities shared template clauses or contracts with OVIC that required CSPs to comply with the PDP Act or the IPPs. **One** university provided a contract that would require a CSP to comply with a number of the IPPs, but not all of them (such as IPPs 1, 3, 5, 8).[9]

98. Some standard form contracts also included clauses requiring "organisational and technical security measures to protect that Personal Information from misuse, loss, unauthorised access, modification and disclosure" and for information to be deleted on termination of the contract.

99. **Five** universities had a process for considering personal information security risks when considering whether to engage a CSP. The processes consisted of:

    a. Conducting PIAs. Some universities noted work carried out to embed PIA processes into project management frameworks and operational processes connected to new initiatives.

    b. Procurement questionnaires and vendor security assessments.

Privacy and information security training

100. OVIC found:

    a. **All** universities conduct training on privacy and information security in the form of online modules such as 'Managing Information & Cybersecurity training', 'Privacy and Data Awareness training'.

    b. In addition, **two** universities provide in person training in some circumstances, such as on request or for high-risk areas.

101. Generally training is delivered to university staff during staff induction. It is not known if other personnel, such as contractors, receive training.

102. **Two** universities require staff to undertake refresher training, every 2-3 years.

[9] For the full text of the IPPs visit Information Privacy Principles - Full Text.

103. Some other awareness raising activities were outlined by universities, such as 'Knowledge Base Articles' available online, activities for Privacy Awareness Week, roadshows with tailored presentations, targeted workshops, or proactive knowledge campaigns.

Observations

104. OVIC's findings in Part 4 of this report are an evaluation of the universities' policies and procedures that support compliance with IPP 4. In developing a framework to assess the universities policies and procedure documents, we considered what is best practice for:

    a. **Updating policies and procedures** – documents are reviewed and updated regularly and according to the review period specified by the university.

    b. **Staff accountability** – clearly defined with key areas of responsibility are assigned and documented.

    c. **Destruction of personal information** – direct readers to consider the purpose of holding the personal information and set out requirements for personnel to consider whether personal information that has been held for a specified period should be destroyed or permanently de-identified.

    d. **Data breach response plans** – response plan covers the key steps and applies to both digital and physical data breaches.

    e. **Sharing personal information with third parties** – policy or procedure sets out when personal information can be shared with third parties and how personal information is protected in those circumstances.

    f. **Engaging CSPs that handle personal information** – third parties are accounted for in risk assessment processes and contracts are used to require compliance with the PDP Act.

    g. **Privacy and information security training** – training is delivered to all university personnel that has access to or handles personal information on behalf of the university.

Recommendations

105. OVIC recommends Victorian universities consider, where they have not already done so:

    a. implementing policies that clearly set out expectations on staff regarding destruction of personal information.

    b. including in data breach response plans a step that requires staff to consider whether notification to OVIC is appropriate.

    c. documenting their approach and requirements when sharing personal information with third parties.

    d. making privacy and information security training available to all personnel that have access to personal information held by the university, including contractors.

PART 5 – Plans for improving information security

106. OVIC asked the universities how they ensure continuous improvement of its personal information security. The universities' responses detailed a variety of ways in which they plan to enhance their security capability.

107. Broadly, Victorian universities appear to be focused on emerging cyber security risks and improving cyber security defences. This focus aligns with a number of media/research articles that explore the increase in phishing and other cyber security attacks on universities in Australia over recent years.

108. A 2020 research article into Australian universities reported that universities are becoming an increasingly attractive target for cybercriminals.10 In particular, Australian National University's data security was at the core of a cyberattack, in which personal data (bank numbers, tax details, academic records and passport details) held by the university was acquired. [11] Officials believe there is growing concern that personal information that is stolen is sold to foreign states. Cybersecurity attacks have the potential to harm individuals and impact on Australian universities' established relationships with stakeholders.[12]

Examination findings

Audits and reviews

109. **Six** universities reported that they had recently undergone or were undergoing audits or assessments on several areas (such as policies, systems) that relate to personal information security. The focus of the audits included:

    a. Privacy policies and procedures.

    b. The elements of the Victorian Protective Data Security Framework (which OVIC oversees under Part 4 of the PDP Act) and its application to the university.

    c. Reviews of cybersecurity, information technology, and physical security – focusing on access, permissions, and the integration of the risk management framework into localised processes within the university.

    d. Security controls to ensure controls align with ISO 27001 (ISO 27001 is an international standard for managing information security.)

110. **Three** universities reported that they had responded or were currently responding (as at November 2020) to the results of their audits. Universities responses to the results included:

    a. Implementing recommendations to improve information security training

    b. Development of a university wide data governance strategy and project, which included a 2020 cyber security strategy.

---

[10] Bongiovanni, I., Renaud, K. and Cairns, G. (2020), 'Securing intellectual capital: an exploratory study in Australian universities', Journal of Intellectual Capital, Vol. 21 No. 3, pp. 481-505.
[11] Michael McGowan (6 June 2019) 'China behind massive Australian National University hack, intelligence officials say', *The Guardian*, accessed 25 May 2021.
[12] Bongiovanni, I., Renaud, K. and Cairns, G. (2020), 'Securing intellectual capital: an exploratory study in Australian universities', Journal of Intellectual Capital, Vol. 21 No. 3, pp. 481-505.

Plans for improvement in the short term

111. OVIC received information about universities' plans to address identified risks and mature processes. These plans generally showed a focus on cyber security, such as plans to implement multi-factor authentication.

    a. One university's plans for improvement related to processes for procuring IT solutions/equipment. This university explained that it plans to further embed Privacy Impact Assessment (**PIA**) process into procurement processes.

    b. Another university said its cyber team and privacy officer jointly released an online tool which consolidates and simplifies the processing of PIAs and ISRAs. The tool has a combined workflow to support integrated assessments.

    c. A third university explained that is has a 'cyber safe' program, which aims to improve the maturity of its vendor management program.

112. OVIC also received details about some short-term plans focusing on data governance, such as:

    a. Work to consolidate existing policies into a new Information Management Policy. The university is aiming for the policy to cover all information managed by the university and cover lifecycle stages.

    b. Redrafting Privacy Guidelines. The university aims to publish the guidelines in 2021 and then aims to integrate the guidelines with new specific IT security guidelines, documents and processes.

Roadmaps and long-term plans

113. Information provided about road maps also showed a strong focus on cyber security. **Six** universities had a cyber security strategy or similar. Roadmaps or similar strategies included:

    a. A cyber security strategy and program of work.

    b. A cyber security strategy for 2020-2022.

    c. An information security compliance framework including a three-year strategic plan, which leverages NIST Cyber Security Framework.

    d. A maturity roadmap that involves an assessment conducted annually against industry benchmarks and internal standards.

114. OVIC found that only **three** universities reported that they have a risk register that is frequently reviewed and includes information security risks. These risk registers are reviewed and updated according to the Risk Management Frameworks. For example, the Information Technology Services area of one university conducts monthly risk workshops. Another university said that its Risk Management Framework is being updated to align with AS/NZS ISO 31000(2018) Risk Management Standards.

Addressing new and emerging risks to personal information security

115. It is common for Victorian universities to be members or attend forums where other universities or organisations share knowledge and collaborate on security practices. These

forums appeared to mostly be about cyber security, to assist universities to keep abreast of the threat landscape.

116. As well as forums, **five** universities referred to their PIA processes when OVIC asked if they had a mechanism identify new and emerging risks to personal information as they arise.[13]

117. At least **two** universities hold frequent internal meetings and conduct biannual compliance reports, between staff such as Risk Manager, Privacy Officer and Senior Manager, Security, Risk and Compliance. This requires one of those staff members to be informed of new and emerging risks to information security and share information with the other staff.

118. OVIC's examination found that some universities may not be addressing emerging risks presented by staff changes (such as new staff or staff movement). Risks could be caused by staff not knowing information handling requirements or reporting structures (such as in the event of a data breach) or personnel checks not being performed where a staff member moves to a role with access to more sensitive information.

Observations

119. PIAs may alert a privacy team to a project that is being considered by a business area that involves new technology. PIAs may not be a useful tool for identifying all risks, such as an increased prevalence of hacking attempts.

120. It is important for risks presented by staff changes or restructures to be addressed because such changes can inadvertently lead to an information security incident. For example, where day-to-day processes are not carried out correctly. Restructures can also raise personnel and physical security risks.

[13] In addition to the five universities who referred to PIA processes in response to this question, other universities referred to their PIA processes throughout the questionnaire.