Australian Government
Australian Sports Commission

ASC Privacy Impact Assessment Microsoft Office 365 and Azure

Table of contents

Executive summary

The ASC Privacy Officer with input from stakeholders has conducted a Privacy Impact Assessment (PIA) on the planned implementation of Microsoft Office 365 and Microsoft Azure in a cloud hosted environment.

The implementation is part of the ASC digital roadmap.

The ASC recognises that implementing cloud based solutions raises potential privacy issues and the requirement to commission a PIA to reflect and consider the major changes in information handling practices.

This PIA considered the following environmental factors:

- The requirement to protect privacy in compliance with Australian privacy legislation and the Australian Privacy Principles
- That the purposes for which the ASC collects, uses and discloses personal information are unchanged within this proposed cloud implementation
- The direction and guidance by the Commonwealth of Australia to agencies to move their systems and storage into the cloud
- The proven capability of Microsoft to provide services which are accredited and certified to meet Australian standards and legislation in regards to security and privacy
- The understanding that the Microsoft cloud environment may be considered more secure than current ASC and externally managed services.

Finding

Microsoft Office 365 and Microsoft Azure appear to comply with the use and disclosure requirements of the APPs in the *Privacy Act 1988* (Cth).

This PIA finds that the risk of privacy harms to ASC held personal information through misuse or inappropriate disclosure through use of Microsoft Office 365 and Microsoft Azure is low to medium and within the ASC risk threshold.

What is a privacy impact assessment?

A privacy impact assessment (PIA) assesses the privacy impacts of new or amended projects or processes. A PIA identifies the ways negative privacy impacts can be mitigated and positive impacts enhanced. PIAs are an important part of the ASC's risk management and planning processes.

The *Privacy Act 1988* requires us to protect 'personal information'.

> **'Personal information'** is defined in section 6 of the Privacy Act as:
>
> information or an opinion about an identified individual, or an individual who is reasonably identifiable:
>
> whether the information or opinion is true or not; and
> whether the information or opinion is recorded in a material form or not.

Common examples of personal information are a person's name, home address, date of birth, medical records or employment details as well as commentary or opinions about a person.

A PIA must be prepared when considering or undertaking the following activities:

- new or existing projects
- changes to processes or procedures
- policy proposals
- initiatives, programs or activities
- new or amended technology, systems or databases
- new procedures involving overseas entities or disclosures of personal information to overseas recipients are being considered.

1. Project/process description

1.1. What is the project or process?

The ASC and Microsoft are proposing to make Microsoft Office 365 and Microsoft Azure services available to the ASC.

This PIA is to consider the privacy considerations stemming from ASC implementation of cloud based Microsoft productivity tools and storage.

The ASC currently hosts its data on premise and in a range of controlled and uncontrolled local and cloud environments. This project is planning on centralising and outsourcing the Microsoft applications and physical storage of ASC data to Microsoft cloud based services. This will involve the transfer of storage (though not ownership or control) of ASC data from the ASC to Microsoft cloud environment. The ASC must balance the benefits and risks and its requirement to protect the personal information of Australians it holds.

In preparing this PIA the following guidance documents have been considered:

- Digital Transformation Agency. *Secure Cloud* at: https://www.dta.gov.au/what-we-do/policies-and-programs/secure-cloud/
- Australian Signals Directorate. *Cloud Computing Security Considerations* at: https://asd.gov.au/infosec/cloudsecurity.htm
- Attorney-General's Department. *Australian Government Information Security Management Protocol* at:https://www.protectivesecurity.gov.au/informationsecurity/Pages/Australian-Government-information-security-management-protocol.aspx
- Office of the Australian Information Commissioner. *Guide to Securing Personal Information* at:https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information
- Office of the Australian Information Commissioner. *Guide to Undertaking Privacy Impact Assessments* at:https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments
- National Archives of Australia. *Cloud Computing and Information Management* at: http://www.naa.gov.au/information-management/managing-information-and-records/storing/cloud/index.aspx

1.2. What are the aims or objectives of the project or process?

The principal aims of the project are to:

- Provide ASC staff with Office productivity and collaboration tools that allow them to work more effectively internally and with external sport partners.
- Enable staff to work anywhere anytime on any device when using Office productivity tools
- Enable internal and external collaboration in real time.
- Enable large scale storage and control of data through a single secure platform
- Reduce IT complexity and operating costs by transferring ASC physical storage and services to Microsoft Cloud services.
- Reduce the overhead of upgrading the Microsoft Office suite internally - Office 365 provides upgrades and new features as they become available.
- Provide collaboration technologies that meet the expectations and needs of staff and ASC partners.
- Reduce up-front capital expenditure on IT data centre equipment.
- Consolidate cloud tools around secure and managed ASC services, substantially offsetting existing risks associated with the broad range of unplanned / unsupported consumer Cloud services currently in-use.
- Improve privacy and security compliance through the reduction of local storage and the use of portable storage devices.

1.3. What is the scope of the project or process?

Implementation of cloud based Microsoft productivity tools and storage and transfer of current ASC IT services from on premise to cloud services.

1.4. Who is responsible for the project/process?

ASC DGM, Business Operations Branch

1.5. If you are making changes to an existing process or procedure, has a PIA already been completed?

No.

1.6. What did the PIA show? What is the current status of the PIA?

Not applicable.

1.7. What type of personal information is involved in the project or process?

See **Appendix A.**

1.8. Does the project/process link to any other existing programs or projects? If so, provide details in the attached table.

Related project	Nature of relationship
Office 365 Implementation	• Implementation of Microsoft Office 365 – Implementation of core Office 365 services (desktop Office applications, Cloud email (Exchange online) and Calendar, OneDrive personal shares, Skype for Business, Yammer, Planner and Microsoft Teams). • Transition existing on-site user data (M: drives and Outlook) to Office 365. • Automated ASC staff account provisioning in Office 365.
Azure Cloud Implementation	Implementation of Microsoft Azure Cloud services – establishing an ASC foundation for future Cloud storage, data services and secure computing.
Dynamics 365	Dynamics 365 is a cloud based Customer Relationship Management system. ASC currently has Dynamics 365 in a sandbox environment. Once Dynamics 365 is migrated to production, integrating Dynamics 365 with Office 365 will allow ASC staff to record meetings, emails, phone calls and tasks with external stakeholders in a single place using Office 365. This allows for ASC staff to have a single view of all interactions with external stakeholders.
Identity Management Implementation	The Identity Management solution will be required to automatically provision the correct Office 365 groups and permission to staff.
Security Remediation	This will determine our legislative requirements for security within our cloud environment. This includes: classification, sharing controls, data holdings etc.

2. Stakeholders

2.1. **Who do you need to consult to identify what personal information will be affected by the project?**

All ASC business areas are affected by this process.

Staff from a range of business areas (including IT, Governance, HR, Marketing, Customer Insights & Analytics, Sport Business, AIS) were consulted in the creation of this Assessment.

2.2. How will the personal information be collected, used, disclosed and stored? (Consider external as well as internal stakeholders.)

The purposes for which the ASC collects, uses and discloses personal information are unchanged within this proposed cloud implementation.

Personal information may be collected directly from the individual about who the information pertains by paper based or online tools. Personal information may also be collected from other government sources, members of the public, private sector or media.

The ASC will continue to utilise Microsoft Office productivity tools to carry out its functions, but will be moving storage to a cloud based service provided by Microsoft. Additionally other information and data currently held by the ASC on premise will be transferring to cloud based storage on the Microsoft Azure service.

3. Handling personal information

3.1. Collecting personal information

APP 2 – anonymity and pseudonymity

When dealing with the ASC, customers must be given the option of not identifying themselves or of using a pseudonym, unless we are required or authorised by law to deal only with identified people, or it is impracticable to deal with someone if we don't know who they are.

APP 3 – collection of personal information

Any personal information we collect (including sensitive information) must be reasonably necessary for, or directly related to, one or more of the ASC's functions or activities.

We cannot collect sensitive information about a person unless they consent and the information is reasonably necessary for, or directly related to, one or more of our functions or activities, or one of the exceptions in APP 3.4 applies.

Personal information can only be collected by lawful and fair means.

Personal information about a person can only be collected from that person, and not from anyone else, unless one of the exceptions in APP 3.6 applies.

APP 5 – notification of the collection of personal information (APP 5)

When we collect personal information we must notify the customer or otherwise ensure they are aware of, the matters listed in APP 5.2. These matters include:

- the ASC's identity and contact details
- the fact and circumstances of the collection (if personal information has been collected from someone other than the person and the person may not be aware of this)
- whether collection is required or authorised by law
- the purposes for which the information is collected
- the main consequences, if any, for the customer if the personal information is not collected
- who the ASC usually discloses the personal information to
- information about the ASC's Privacy Policy – how customers can access and correct their personal information and how they can complain about a breach of their privacy
- whether the ASC is likely to disclose personal information to people or organisations overseas and if so, the countries in which those people or organisations are located (if practicable).

3.1.1 What personal information, including sensitive information, will be collected? Where will the information come from? What is the sensitive information?

The ASC collects a range of types of personal and sensitive personal information. These are listed at Appendix A.

The intent of the project is to over time transition all current ASC collection and storage of personal information into a cloud based Office 365 and/or Azure storage environment.

The ASC may collect sensitive information when:

- providing health services to persons (for example to an athlete)
- conducting sport research

- it is required to provide specific services (for example in allocating specifically targeted funding)
- assessing eligibility for employment (potential or existing employees)
- for the purpose of maintaining the employee/employer relationship
- for the purpose of meeting legal employment obligations

3.1.2 Is the personal information necessary for, or directly related to, one or more of the ASC's functions? Provide details.

Yes.
The ASC is Australia's primary national sports administration and advisory agency, and the cornerstone of a wide-ranging sports system. On behalf of the Australian Government, the ASC delivers key programs in line with the Australian Government's sport policy objectives.

The ASC's activities and services include:

- Conducting sports science and research
- Providing medical, social and material support to athletes
- Providing sports information and education
- Delivering funding programs to sporting organisations and individuals
- Supporting sporting participation development
- Managing sporting facilities

A potential threat to privacy is Office 365 users collecting more personal information than is necessary for them to perform their function. Office 365 provides software services and a repository, it does not automatically impose any control over the content of the information which a user collects and stores. The personal information that a user is able to collect is potentially limitless. However, the ASC is able to build business rules into Office 365 and Azure which can identify and alert the ASC to personal information holdings.

3.1.3 Does the ASC already have the personal information? (For example, was it collected in relation to a different function or activity?)

Yes. The ASC already holds a range of types of personal information. The functions and activities for which it gathers and manages personal information are unchanged within this proposed cloud implementation.

3.1.4 Is collection of this personal information authorised or required by the ASC by legislation?

Yes. The ASC requires a range of personal information to be collected and managed for the purposes of delivering services to Australians and to sporting organisations under the functions of the *Australian Sports Commission Act, 1989* (Cth).

3.1.5 Will the personal information be collected by lawful and fair means?

Yes.

3.1.6 How will the personal information be collected?

At the ASC, personal information is collected through:

- Online (web) forms
- Online surveys
- Online messaging
- Calendar
- Emails or email attachments
- Documents uploaded to collaboration portals (e.g. Word, Excel)
- Paper forms
- mobile apps (applications)
- over the telephone
- in person contacts
- medical examinations, testing or sensing systems
- sport testing or sensing systems
- online video and messaging services
- CCTV surveillance
- Shared sports systems

Any other form of communication or data transfer may also be used by the ASC to collect personal information.

3.1.7 Will customers have the option of not identifying themselves or of using a pseudonym? If not, why not?

Depending on the nature of a person's relationship with the ASC, they may not need to personally identify themselves. ASC online information collection forms do not have mandatory personally identifying fields.

Persons generally have a right to pseudonymity or anonymity when dealing with the ASC, unless:

- the ASC is required or authorised by or under an Australian law, or a court/tribunal order to deal with individuals who have identified themselves;
- it is impracticable to deal with individuals who have not identified themselves; and
- the person is receiving a service or financial benefit from the ASC - which necessitates assurance that the service or monies is being directed to an identified person.

ASC staff do not have the option of not identifying themselves (though staff may request a 'work name'). Staff must maintain an Office 365 account to facilitate information exchanges and emails. As a result Office 365 will contain user account information and audit logs for ASC staff.

3.1.8 Who will provide the information? (Will the subject of the information provide it, or will it be provided by a third party, such as a business or organisation?)

Where it is reasonable and practical to do so, the ASC will collect personal information directly from the persons concerned with their consent.

In some circumstances personal information about an individual will be provided by a third party such as a National Sporting Organisation.

3.1.9 If the information will come from a third party, do any of the exceptions in APP 3.6 apply?

The ASC may need to collect personal information from other people or organisations – in particular from sporting organisations. This information is expected to be collected with the person's consent, except for in circumstances allowed for by legislation. Sometimes this may happen without direct involvement. Some examples of the people or organisations from which the ASC may collect personal information about persons are:

- sporting organisations
- medical professionals
- publicly available sources of information (such as directories or websites)
- person's representatives (such as a parent, coach, legal adviser, manager)
- person's employers
- other government agencies
- law enforcement agencies

3.1.10 If the information comes from a third party, would the subject of the information be aware that the ASC has collected their personal information?

Yes. The ASC generally only collects personal information directly from the person or their representative. Where the ASC collects personal information from third parties it is sourced from reliable and trusted sources (such as National Sporting Organisations or other Commonwealth or State or Territory agencies). The ASC would expect the supplying third party to have sought prior consent or at a minimum have notified the affected individual.

The ASC makes a reasonable attempts to confirm that prior consent has been given, before collecting information from a third party.

3.1.11 If the customer would not be aware the ASC will or has collected their personal information, how and when will a collection notice (which lists the matters in APP 5.2) be given?

Not applicable

3.1.12 How often will the personal information be collected (once only or will it be ongoing)?

Subject to the purpose, function or service being supplied, the ASC may collect personal information both once only and ongoing.

3.2. Using and disclosing personal information

APP 6 – use or disclosure of personal information
The ASC can only use or disclose personal information for the purpose for which it was collected (the 'primary purpose'). Personal information cannot be used or disclosed for another purpose ('secondary purpose') unless the person consents or one of the exceptions in APP 6.2 applies.

APP 8 – cross-border disclosure of personal information
If the ASC discloses personal information to someone overseas we are accountable for any privacy breaches committed by the overseas person or organisation (see s. 16C of the Privacy Act).

Therefore, before we disclose personal information to a person or organisation overseas, we must take reasonable steps to ensure they do not breach the APPs in relation to the information, unless one of the exceptions in APP 8.2 applies.

For each business unit/contracted service provider involved in the project, consider the following:

3.2.1 What personal information, including sensitive information, will be used or disclosed? (Include both planned and infrequent uses)

The types of personal and sensitive information and its planned ASC uses and disclosures of personal information are unchanged within this proposed cloud implementation.

The ASC will use personal information only in relation to its functions and for the purposes of delivering services to Australians and to sporting organisations. This may include Microsoft and the ASC using all types of personal information held by the ASC.

The ASC will utilise Microsoft Office cloud productivity services to carry out its functions and will be moving storage to a cloud based service. Additionally other information and data held by the ASC will be transitioning to cloud based storage on the Microsoft Azure service. Effective ownership and control of ASC owned personal information will be retained with the ASC.

3.2.2 For what purpose(s) will the personal information be used or disclosed?

The purposes for which the ASC uses and discloses personal information is unchanged within this proposed cloud implementation.

The ASC will utilise Microsoft Office cloud productivity services to carry out its functions and will be moving its storage to a cloud based service. Additionally other information and data held by the ASC will be transferring to cloud based storage on the Microsoft Azure service. The ASC considers storage of personal information on Microsoft contracted services constitutes use and not disclosure.

3.2.3 Are these purposes directly related (sensitive information) or related (non-sensitive information) to the purpose for which the personal information was originally collected? (Why was the information originally collected?)

Yes. The ASC collects personal information for the purposes of delivering services to Australians and to sporting organisations under the functions of the *Australian Sports Commission Act, 1989* (Cth). The ASC will allow Microsoft use of the personal information and data for the purpose of providing services to the ASC for the ASC to complete its functions. Office 365 will provide the ASC with the following capabilities; email, calendar, directory, instant messaging, collaboration space, planning, Skype for Business, Microsoft Productivity suite (Word, Excel, PowerPoint, Access and OneNote). These capabilities facilitate official communications and allow staff and external parties to share information electronically. Effective communication is essential to the ASC delivering its functions under the *Australian Sports Commission Act, 1989.*

3.2.4 If the personal information will be used for a secondary purpose, consider whether you will ask the customer to consent to it being used for that purpose? Where will you file a record of their consent?

In accordance with the ASC Privacy Policy, where the ASC may seek to use information for a secondary purpose it will seek additional consent. Where appropriate any secondary consent will be held with the information and/or in the ASC EDRMS.

3.2.5 If the information will be used for a secondary purpose and the customer will not be asked for consent, do any of the exceptions to the requirement for consent in APP 6.2 apply?

Not applicable.

3.2.6 To whom will the personal information be used or disclosed? How will it be disclosed?

The purposes for which the ASC uses, and the parties to which the ASC discloses personal information is unchanged within this proposed cloud implementation.

Any form of disclosure will be dependent upon the service or function undertaken by the ASC.

Through this project, the ASC will allow Microsoft use of ASC personal information only for the purposes of delivering services to the ASC. Effective ownership of ASC owned personal information will be retained with the ASC.

3.2.7 What measures are in place to prevent the personal information being used in a way that is not permitted under the APPs?

The purposes for which the ASC uses, and the parties to which the ASC discloses personal information is unchanged within this proposed cloud implementation.

The ASC has policy and technical controls to ensure that personal information is used as permitted under the APPs.

The ASC will have contractual obligations in place with Microsoft to ensure ASC owned personal information is used or accessed only for the purposes of delivering services to the ASC.

3.2.8 If personal information is to be disclosed to a person or organisation overseas, will reasonable steps be taken to ensure they do not breach the APPs in relation to the information?

Yes. The parties to which the ASC discloses personal information is unchanged within this proposed cloud implementation.

The ASC considers that providing personal information to an overseas services provider is a use, rather than a disclosure (APP Guidelines 8.14).

Within this proposal through contractual obligations with Microsoft the storage of ASC data in Microsoft Azure and where possible for Office 365 will be retained and managed within data centres in Australia. There is an understanding that Azure data will reside only in Australia Central and Australia Central 2 (https://azure.microsoft.com/en-au/global-infrastructure/australia/).

At the time of this PIA it is understood the following Office 365 services are hosted in Australia:

- Exchange Online
- OneDrive
- SharePoint Online
- Skype for Business
- Project Online
- OneNote.

At the time of this PIA it is understood the following Office 365 services may be hosted overseas:

- Teams (Hong Kong, Singapore, South Korea)
- Sway (United States)
- Planner (Hong Kong, Singapore)
- Yammer (United States)

The ASC intends to use these overseas hosted services – noting that these services are not services that the ASC would normally hold sensitive (e.g. medical, personnel) personal information.

Where the ASC uses overseas hosted services, it will consider use only where the nations that Microsoft may host data are subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way the APPs protect information and mechanisms can be accessed by the individual to enforce that protection of the law or binding scheme (APP Guidelines 8.19). The ASC considers that the USA, Hong Kong, Singapore, and South Korea (all members of APEC and APPA) enforce a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way the APPs protect the information, and for which mechanisms can be accessed by the individual to enforce that protection of the law or binding scheme.

3.2.9 If not, does an exception under APP 8.2 apply? If no exception applies, are appropriate arrangements in place to ensure that personal information is handled in accordance with the APPs?

Not applicable.

3.2.10 Is there any intention or potential for personal information to be data-matched, linked or cross-referenced to other information held in different databases (by you or other entities)?

The functions or services of the ASC are unchanged within this proposed cloud implementation.

The ASC expects to data-match, link or cross-reference personal information currently held in its own databases. This activity will be conducted within the Microsoft Azure and Office365 environments.

The ASC may data-match, link or cross-reference personal information currently held in its own databases with data held by Australian sporting organisations. This activity may be conducted within the Microsoft Azure and Office365 environments. This activity will occur only where permission has been granted.

3.3. Information quality

APP 10 – quality of personal information

The ASC must take reasonable steps to ensure that the personal information we collect, use and disclose is accurate, up-to-date and complete.

3.3.1 What steps will be taken to ensure that any personal information collected is accurate, up-to-date and complete?

The steps and activities that the ASC undertakes to ensure that the personal information collected is accurate, up-to-date are unchanged within this proposed cloud implementation.

3.3.2 What steps will be taken to ensure that any personal information used or disclosed is accurate, current, complete and relevant (having regard to the purpose of the use or disclosure)?

The ASC seeks to maintain the quality of its information holdings by taking reasonable administrative and technical steps to make sure that the personal information held is accurate, complete and up-to-date.

3.3.3 What are the consequences for customers if the personal information used or disclosed as part of the project is not accurate or up-to-date?

Inability to deliver functions or services as expected.

3.3.4 Will customers be given the opportunity to correct or update their personal information before we collect, use or disclose it?

Any person who believes that the ASC holds personal information about them may contact the agency to seek access to that information in accordance with APP 12.

If after accessing information held about any person, they consider that it is inaccurate, out-of-date, incomplete, irrelevant or misleading for the purposes for which it is held, then they may request the ASC to amend it in accordance with APP 13.

In the first instance a person can request access to their personal information by contacting the ASC.

3.4. Data security

APP 11 – security of personal information

The ASC must take reasonable steps to protect the personal information we hold from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

3.4.1How will the personal information be stored (for example, on a paper file, digitally on the ASC's servers or an external (cloud) data storage facility)?

Personal information will be stored digitally on an external cloud data storage facility located in Australia and managed by Microsoft Australia.

3.4.2 Will reasonable steps be taken to ensure technical and physical security is in place to protect against misuse, interference and loss?

Yes. The ASC has considered the reasonable steps to include:

- retention of ownership of the information and the ability to control access to the information
- contractual measures and protections to ensure that information is safeguarded and secure and privacy is protected
- contractual measures to ensure a suitable vetting process for all staff who will have access to ASC systems and/or information
- contractual measures to audit the vendor's compliance with those security arrangements

The ASC considers that there is minimal risk of privacy harms through misuse, interference or loss of personal information collected or retained within Office 365 and Azure by vendor action or inaction.

Microsoft sets out the security and privacy certifications and compliances met by Office 365 at: https://products.office.com/en-au/business/office-365-trust-center-compliance-certifications

Microsoft sets out the security and privacy certifications and compliances met by Azure at: https://azure.microsoft.com/en-au/overview/trusted-cloud/

Within Australia, certain Microsoft Azure and Office 365 services have been accredited for the Certified Cloud Services List (CCSL), which identifies cloud services that have successfully completed an Information Security Registered Assessors Program (IRAP) assessment by the Australian Signals Directorate (ASD).

As of April 2018 Azure and Office 365 cloud services are accredited by the ASD for information/data up to the Classification level of PROTECTED (see https://www.asd.gov.au/infosec/irap/certified_clouds.htm).

It should be noted that the ASC currently operates in an Unclassified (Official) environment.

The ASC considers that Microsoft:

- has the appropriate level of security to safely manage ASC data
- complies with all Australian laws generally applicable to its services
- is expected to comply with the privacy and security contractual obligations entered into with the ASC
- will not require any rights in ASC data
- will only use or disclose ASC data for the following purposes :
    - to provide the ASC with the Office 365 and Azure services,
    - where required by law, for law enforcement purposes

- will define and follow its approach to transfer and deletion of ASC data on termination of ASC's use of Microsoft Office 365 and/or Azure.
- personnel will not process ASC data without authorisation and are obliged to maintain the confidentiality of any ASC data.

3.4.3 Will reasonable steps be taken to ensure that the personal information is protected from unauthorised access, modification or disclosure?

Yes. The ASC has considered the reasonable steps to include:

- security arrangements to ensure access controls, audit logging and other treatments or controls are implemented to prevent unauthorised access to personal information
- controls to ensure notification and reporting of any information breaches found to have occurred
- contractual measures to ensure a suitable vetting process for all staff who will have access to ASC systems and/or information
- contractual measures to audit the vendor's compliance with those security arrangements

The ASC considers that there is minimal risk of privacy harms through unauthorised access, modification or disclosure of personal information collected or retained within O365 and Azure by vendor action or inaction.

Microsoft sets out the security and privacy certifications and compliances for Office 365 at: https://products.office.com/en-au/business/office-365-trust-center-compliance-certifications

Microsoft sets out the security and privacy certifications and compliances for Azure at: https://azure.microsoft.com/en-au/overview/trusted-cloud/

Within Australia, Microsoft Azure and Office 365 are accredited for the Certified Cloud Services List (CCSL), which identifies cloud services that have successfully completed an Information Security Registered Assessors Program (IRAP) assessment by the Australian Signals Directorate (ASD).

As of June 2018 Azure and Office 365 cloud services are accredited by the ASD for information/data up to the Classification level of PROTECTED (https://www.asd.gov.au/infosec/irap/certified_clouds.htm). It should be noted that the ASC operates in an Unclassified (Official) environment.

The ASC considers that Microsoft:

- has the appropriate level of security to safely manage ASC data
- complies with all Australian laws generally applicable to its services
- is expected to comply with the privacy and security contractual obligations entered into with the ASC
- will not require any rights in ASC data
- will only use or disclose ASC data for the following purposes :
    - to provide the ASC with the Office 365 and Azure services,
    - where required by law, for law enforcement purposes

- will define and follow its approach to transfer and deletion of ASC data on termination of ASC's use of Microsoft Office 365 and/or Azure.
- personnel will not process ASC data without authorisation and are obliged to maintain the confidentiality of any ASC data.

3.4.4 Will control procedures be in place requiring authorisation before personal information is added, changed or deleted?

The controls and access provisions for ASC staff that the ASC utilises are unchanged within this proposed cloud implementation. Noting that the ASC will continue to use Active Directory (except now cloud hosted). ASC staff will continue to have access to information limited by the access required for their role and ASC access controls.

Contractual obligations on Microsoft, are entered into to ensure Microsoft personnel will not add, change or delete ASC data without ASC authorisation.

3.4.5 Who will have access to the personal information? Who will authorise access?

The controls and access provisions to personal information for ASC staff and authorised third parties are unchanged within this proposed cloud implementation.

ASC Managers will be required to provide authorisation before staff or authorised third parties have access to personal information.

ASC staff or authorised third parties will have access to personal information only where there is a specific business requirement.

ASC controlled Medical (Sensitive) personal information may only be accessed by medical staff, or where otherwise given consent by the patient or their representative.

Contractual obligations on Microsoft, are entered into to ensure Microsoft personnel will have access to ASC held personal information only to provide the ASC with Office 365 and Azure services.

Authorisation to provide Microsoft with access to ASC held personal information will be made by the ASC Executive, and communicated through the ASC DGM, Business Operations Branch.

3.4.6 Will audit mechanisms identify inappropriate system access?

Yes.
Microsoft Office 365 and Azure offer the ability to monitor suspicious activity with reporting, auditing, and alerts, and to mitigate potential security issues.

For the ASC to be able to have the required audit mechanisms in Microsoft Office 365, it will need to consider engaging Enterprise Mobility Suite (EMS) E3 licences for all staff.
The EMS E3 license has base level audit control for Office 365, but does not have the ability to audit actions taken by admin staff. To perform this audit action senior admin and security staff would require EMS E5 licences.

3.4.7 If the personal information is being managed by an external provider, how will it be protected?

The ASC in accordance with APP11 undertakes to take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

The ASC determines that the external provider (Microsoft) will have physical possession of ASC held personal information, but that the ASC retains effective control and ownership.

The ASC considers that Microsoft Office 365 and Azure offer a range of security protections that meet the ASC's requirements to protect the personal information in its possession.

Microsoft sets out the security and privacy certifications and compliances for Office 365 at:
https://products.office.com/en-au/business/office-365-trust-center-compliance-certifications

Microsoft sets out the security and privacy certifications and compliances for Azure at:
https://azure.microsoft.com/en-au/overview/trusted-cloud/

Within Australia, certain Microsoft Azure and Office 365 services are accredited for the Certified Cloud Services List (CCSL), which identifies cloud services that have successfully completed an Information Security Registered Assessors Program (IRAP) assessment by the Australian Signals Directorate (ASD).

As of April 2018 Microsoft Azure and Office 365 cloud services are accredited by the ASD for information/data up to the Classification level of PROTECTED (https://www.asd.gov.au/infosec/irap/certified_clouds.htm). It should be noted that the ASC operates in an Unclassified (Official) environment.

The ASC considers that Microsoft:

- has the appropriate level of security to safely protect ASC data
- complies with all Australian laws generally applicable to its services
- is expected to comply with the privacy and security contractual obligations entered into with the ASC
- will not require any rights in ASC data
- will only use or disclose ASC data for the following purposes :
    - to provide the ASC with the Office 365 and Azure services,
    - where required by law, for law enforcement purposes

- will define and follow its approach to transfer and deletion of ASC data on termination of ASC's use of Microsoft Office 365 and/or Microsoft Azure.
- personnel will not process ASC data without authorisation and are obliged to maintain the confidentiality of any ASC data.

3.4.8 Does the project comply with the ASC's information security documented controls?

Yes. The ASC implementation of Microsoft Office 365 and Microsoft Azure will be managed in accordance with current ASC security documents and controls.

3.4.9 Does the project adopt the recommendations of the OAIC's Guide to information security?

Yes. The procurement and implementation of Microsoft Office 365 and Microsoft Azure adopts the recommendations in a number of ways including but not limited to completing this PIA and having governance and technical arrangements in place for the secure collection, storage, updating and deletion of personal information.

3.4.10 Does the project comply with the ASC's Records Policy and Records Authority?

Yes. The ASC Records Authority and policies are unchanged within this proposed cloud implementation.

The ASC implementation of Office 365 and Azure will ensure records (including personal information) will be kept be for the applicable retention periods. Effective ownership of ASC records will be retained with the ASC.
The ASC EDRMS (Content Manager) is unchanged in the initial transfer of services and storage to cloud services.

3.5. Access and correction

APP 12 – access to personal information

When the ASC holds personal information about a person, we must give them access to it on request (unless we are required or authorised to refuse access under the *Freedom of Information Act 1982* or another Commonwealth law that provides for access to documents).

APP 13 – correction of personal information

The ASC must take reasonable steps to correct personal information to ensure it is accurate, up-to-date, complete, relevant and not misleading.

This requirement applies when:

- the ASC is satisfied the information is inaccurate, out-of-date, incomplete, irrelevant or misleading, having regard to the purpose for which it is held, or
- the person asks the ASC to correct the information.

The minimum procedural requirements for correcting personal information require the ASC to:

- take reasonable steps to notify other agencies that personal information we have previously disclosed to them has been corrected (if the person asks us to)
- give the customer a written notice within 30 days setting out the reasons for refusal and the complaint mechanisms available to them (if correction is refused)
- take reasonable steps to associate the information with a statement that it is inaccurate, out of date, incomplete, irrelevant or misleading (if correction is refused)
- not charge for making a request for correcting personal information or for associating a statement with the personal information.

3.5.1 How can customers access their personal information?

Any person can request access to their personal information by contacting the ASC.

3.5.2 Who will be responsible for responding to requests for access to or correction of personal information?

ASC Privacy Officer
Australian Sports Commission
PO Box 176 Belconnen ACT 2616
privacy@ausport.gov.au

3.5.3 How can customers update their personal information, or have annotations made, if necessary?

If after accessing information held about any person, they consider that it is inaccurate, out-of-date, incomplete, irrelevant or misleading for the purposes for which it is held, then they may request the ASC to amend it in accordance with APP 13.
In the first instance a person can request access to their personal information by contacting the ASC.

3.5.4 How will decisions be made about requests from customers for access to or correction of their personal information?

The ASC Privacy Officer will make decisions on access. The ASC privacy Officer in coordination with the relevant business area will make decisions on the correction of personal information. Where any decision is found unsatisfactory to the applicant, escalation will occur as necessary.

4. Privacy management

4.1. Identifying and addressing the risks

Go through your responses to 3.1 to 3.5 to identify and analyse the privacy risks.

What can you do to do remove, minimise or mitigate the negative privacy impacts identified?

Strategies to reduce or mitigate privacy risks include:

- technical controls (for example, access control, encryption, design changes)
- operational controls (policies or procedures, staff training, oversight and accountability measure
- communication strategies (privacy notices).

The Australian Information Commissioner's 'Guide to undertaking privacy impact assessments' has a list of possible mitigation strategies for common privacy risks which you might like to consult.

Assess whether the privacy safeguards we currently have in place will be sufficient to protect the personal information handled in the project.

Privacy Risk	**Suggested mitigation strategy**
Unauthorised access or disclosure through vendor	Contractual obligations on Microsoft that ensure confidentiality and privacy. Contractual obligations on Microsoft to ensure breach notification and where necessary rectification and recovery. Contractual obligations on Microsoft to ensure security controls including: • Restriction of physical data centre access to authorised personnel. Multiple layers of physical security, such as biometric readers, motion sensors, 24-hour secured access, video camera surveillance, and security breach alarms. • Encryption of data both at rest and via the network as it is transmitted between a data centre and a user • Regular back-up of data • Data portability at the end of contract • Data hosting in Australia or countries that are subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is

	at least substantially similar to the way the APPs protect information • Enforced passwords.
Unauthorised access or disclosure through ASC, a contractor or third party.	Staff and contractor privacy education and training. Technical controls to limit and monitor access to personal information. Microsoft automated detection and intrusion notification to ASC. Regular check of audit logs to review and monitor access and use of personal information. Senior admin and security staff have appropriate access and capabilities to manage audit role (e.g. EMS E5 licences). Implement role based access within Office 365 and Azure commensurate with the users need to access information and tools. Enterprise mobility management to prevent unauthorised access to personal information on staff mobile devices. Pre-employment checks on staff suitability and criminal history. Vetting of key ASC staff though the Australian Government Security Vetting Agency. ASC staff to maintain security access to ASC systems, by: o Using passwords of required complexity o Not storing or sharing passwords o Removing password access where appropriate o Securing computers o Two-factor authentication when working on a non-ASC device. Privacy training and education for ASC staff. ASC Code of Conduct and ASC Privacy Policy. ASC breach notification procedures.

	Contractors sign contracts confirming they will use ASC systems within acceptable use guidelines and be bound by the Privacy Act.
Loss of personal information through vendor action or inaction	Contractual obligations on Microsoft that ensure security and recoverability from loss. Microsoft back-up policies and procedures. ASC back-up policy and procedure.
Collection of personal information unnecessary for the services or functions of the ASC.	Privacy training and education for ASC staff. Privacy notices on all electronic data collection forms.

4.2. Identifying and addressing the risks

Refer to the ASC's Risk Management Policy and complete the risk matrix below. It may be appropriate to add the significant risks identified in this PIA to the ASC's Risk Register. List your action items arising from your analysis above, including who is responsible for the action and the timeframes that apply.

Risks have been defined according to the ASC Risk Levels at Appendix B.

Risk	Consequence	Likelihood	Initial Risk Rating	Risk Mitigation Strategy	Final Risk Rating	Risk Owner
Changes in Commonwealth information security policy in relation to use of cloud storage	Major. ASC is required to cease using external cloud services. ASC is required to raise its Classification level.	Rare	Low	ASC as CCE agency may opt out of ISM/PSPF controls, where it has considered and accepted the risks. If required by Commonwealth direction the ASC may seek	Low	CEO / ASC DGM, Business Operations Branch

				to utilise Office 365 and Azure tools to enable Classification markings and use Microsoft Australian Government Cloud services that are certified at the PROTECTED level		
A privacy breach occurs	Moderate. Unauthorised disclosure of personal information occurs. Harm to Australians. Reputational damage to the ASC. Financial implications for the ASC.	Possible	Medium	Microsoft security processes and systems. ASC IT security processes and systems. Ongoing staff training and education in privacy. ASC privacy breach procedures.	Medium	CEO / ASC DGM, Business Operations Branch
The discovery that controls are not operating effectively or as expected	Moderate. Possibility of unauthorised disclosure of personal information is identified.	Possible	Medium	Microsoft security processes and systems. ASC IT security processes and systems. Ongoing staff training and education in privacy.	Medium	ITSA / ASC DGM, Business Operations Branch
The occurrence of a cyber security incident,	Moderate. Unauthorised third party access gained to ASC data.	Possible	Medium	ASC ITSA manages IT security in an ongoing capacity.	Medium	ITSA / ASC DGM, Business Operations Branch

directly or indirectly	Possible unauthorised disclosure of personal information occurs. Possible harm to Australians. Reputational damage to the ASC. Financial implications for the ASC			Microsoft security and response capability is functional. Recovery and continuity procedures are effective.		
Loss of personal information through accidental or intentional deletion or corruption of data, system failure or disaster	Major. ASC is unable to provide its services or carry out its functions.	Rare	Low	Microsoft security and response capability is functional. Recovery and continuity procedures are effective. ASC Business Continuity Planning.	Low	ASC DGM, Business Operations Branch
Vendor business failure	Major. Microsoft is unable to supply services. ASC is unable to provide its services or carry out its functions.	Rare	Low	ASC Business Continuity Planning.	Low	ASC DGM, Business Operations Branch
Disclosure of personal information about ASC staff to external vendors, contractors,	Minor	Unlikely	Low	Access controls are in place. Contractual agreements are in place with all external third parties who may	Low	ASC DGM, Business Operations Branch

partner organisations or third parties.				use or access ASC information.		

5. Recommendations

A number of recommendations may emerge from the information entered above.

Recommendations should identify avoidable impacts or risks and how they can be removed or reduced to a more acceptable level. List the action items arising from your analysis above, including who is responsible for undertaking the action and the timeframes.

Recommendation	Who is responsible	Owner	Timeframe
Ensure contractual obligations are adequate and fully address ASC privacy concerns and Australian privacy legislation (specifically APPs)	Director, Projects and Sourcing	ASC DGM, Business Operations Branch	July-Sept. 2018
ASC has advice to assure purchase of Office 365 and Azure products and additions to enable IT security and threat protection as appropriate	ASC ITSA	ASC DGM, Business Operations Branch	July-Sept. 2018
Ensure that Microsoft continues to comply with its security and privacy undertakings and certifications	ASC ITSA	ASC DGM, Business Operations Branch	Ongoing
Ongoing privacy training and education to ASC staff – as mandated under the Australian Government Agencies Privacy Code.	ASC Privacy Officer	ASC DGM, Business Operations Branch	Ongoing
Update ASC Privacy Policy and procedures in relation to cloud based services.	ASC Privacy Officer / ASC Corporate Counsel	ASC DGM, Business Operations Branch	Aug.-Sept. 2018
Ensure IT staff are trained and equipped to manage IT services through cloud services	ICT Director	ASC DGM, Business Operations Branch	Ongoing

6. Respond and review

A PIA is part of an ongoing process of assessment and review; it does not end with preparation of a document.

It is important to respond to the recommendations made and to continue to review and update your PIA. You may decide not to implement all of the recommendations. However you need to document what recommendations you intend implementing (or have already implemented) as well as those you do not intent to implement and the reasons for this.

It may be helpful to implement a plan for implementing the recommendations, including a specific timeframe for remedying or mitigating the risks that have been identified and who is responsible for the implementation.

Version	Created by	Originating programme	Approved by	Date	Revision date	CM reference
0.1	Edgar Crook Privacy Officer	Governance and Compliance	Position title	June 2018		2018/030433/D
1.0	Edgar Crook Privacy Officer	Governance and Compliance	DGM Corporate	6 Dec. 2018		2018/030433/D
1.1	Position title	Division or program	Position title	XX Month 2016	XX Month 2016	XXXX XXXX