Australian Government
Geoscience Australia

Privacy Threshold Assessment

Project Details

Project name	Security Awareness Training Platform
Business owner	Director, Cyber Security
Threshold assessment drafter	Technical Manager ICT Security
Description of the project	The Cyber Security team is implementing a security awareness training program utilising a training platform (Mimecast). The platform provides short video training modules that inform users about different aspects of cyber security. User sentiment and comprehension are measured and recorded via short quizzes. In addition to the training, there is the ability to run simulated phishing campaigns and record the results of these (i.e. which users clicked on links). These help to measure effectiveness of our program and provide further practical experience to users to consolidate knowledge.
Types of personal information being handled as part of the project	Users' names, email addresses and which team they are working in will be stored. In addition their training completion results and the results of phishing simulations.
What is the purpose of handling the personal information?	The users' email addresses will be used to assign training and target phishing simulations. A users' team will be used to make simulations and content more relevant to each individual's work duties. The organisational structure will also allow for aggregated training and testing results to be generated and shared with relevant internal stakeholders. The results will be used to measure the effectiveness of the training, and to target further training to reduce the overall risk profile of the organisation. Controls which are relevant to the handling of this data, and minimise the privacy risk include: • Users are already made aware that their usage of the Geoscience Australia network will be monitored, and are asked to accept this prior to each time they log on. • There will be staff communications regarding the introduction of the new system, which will include mention of phishing exercises. • Results of individuals who have been caught out by simulated phishing emails will only be used for aggregated reporting to internal stakeholders and targeting of training via automated means. Only a limited number of administrators will have access to individual results and these will not be disseminated as a matter of course. • The training platform hosts content in Australia and in the USA on Amazon Web Services. There are specific clauses in the user agreement that state that all ownership of customer data remains with the customer and that any data will be promptly deleted upon

	request. The USA’s privacy legislation affords substantially similar protections to Australian privacy legislation. The company website includes detailed information on Mimecast’s compliance with the European General Data Protection Regulation (https://www.mimecast.com/company/mimecast-trust-center/gdpr-center/technical-organizational-measures/at1/).
Stakeholders	• Security team and executive – own the system and require information on Geoscience Australia’s cyber awareness and maturity. • GA staff – participants in the training, and benefit from the increased security awareness by a reduction in the risk of disruption due to cyber incidents.

Part 1: Personal information handling

Does the project involve new or changed ways of handling personal information?

☑ **Yes** Complete Part 2 of the assessment below.

☐ **No** It is not necessary to complete a privacy impact assessment (PIA).
Record the decision at Part 3 and file this assessment with the Privacy Officer.

Part 2: Determining potential for a high privacy risk

Consider the following questions and record each answer as ‘yes’, ‘potentially’ or ‘no’. The purpose of these questions is to you help you screen for factors which point to the potential for a high privacy risk project. It’s important to note that these questions are non-exhaustive, and you should also consider whether there are any other relevant factors that may indicate that your project is a high privacy risk project.

Will the project involve:	Yes	Potentially	No
Handling large amounts of personal information? *Consider the amount of personal information and the number of individuals that will be impacted by your project. Even if you consider that each individual will only have a small chance of suffering a negative impact, handling personal information on a large scale can increase the privacy risk associated with your project. You should also consider whether your project will result in significant increases in the volume of personal information being handled through new or existing channels.*	☐	☐	☑
Handling sensitive personal information? *Sensitive personal information includes, but is not limited to, information about an individual’s racial or ethnic origin, political opinions, religious beliefs or affiliations, criminal records, sexual preferences or practices, biometric information, health information and genetic information.* *The privacy risk associated with your project can increase if sensitive information is involved given the potential for adverse consequences for an individual, or those associated with the individual, if it is mishandled (for example, discrimination, mistreatment, humiliation or embarrassment).*	☐	☐	☑

Will the project involve:	Yes	Potentially	No
Sensitivities based on the context in which the project will operate? *Consider the context and circumstances surrounding the project. Are there prior concerns over this type of handling or activity? Is the project likely to have community support? Is the handling of personal information novel in any way? What is the current state of technology in this area and has there been any previously identified security or technology flaws? Are there any current issues of public concern that you should factor in? What is the nature of your relationship with individuals that may be impacted by the project? How much control will they have over the handling of their personal information? Would they expect you to use their personal information in this way?*	□	□	☑
Handling personal information in a way that could have a significant impact on the individuals concerned? *Consider the potential consequences for the individuals concerned. For example, negative impacts on physical and mental wellbeing, reduced access to public services, discrimination, and financial loss or identity theft.*	□	□	☑
Disclosing personal information outside of your entity? *Consider whether your project will involve sharing personal information with another entity, organisation or to any individuals other than the individual to whom the information relates. This might include the use of contractors or sub-contractors. Also consider whether your project will require the disclosure of personal information overseas.*	□	□	☑
Handling personal information of individuals who are known to be vulnerable? *Consider whether the activity may have greater sensitivities or disproportionate impacts on vulnerable populations and certain groups of individuals. This could include children and seniors, people with impaired intellectual or physical functioning, people who are not native speakers of the local language, people with low levels of literacy or education, people from a low socio-economic background, people experiencing financial hardship, people who are Aboriginal or Torres Strait Islanders.* *An individual's circumstances, or the increased power imbalance between the individual and an entity, may mean, for example, they are unable to easily consent to, or oppose, the handling of their personal information, understand its implications, or exercise control over their personal information.*	□	□	☑
Using or disclosing personal information for profiling or behavioural predictions? *This includes valuation or scoring, profiling and predicting (including in relation to economic situation, health, personal preferences or interests, reliability or behaviour, location or movements).*	□	□	☑

Will the project involve:	Yes	Potentially	No
Using personal information for automated decision-making? *This might include the use of artificial intelligence technologies or data analytics techniques on personal information to produce insights for policy-making or improved service delivery. It might also include using automated decision-making to make decisions that affect the rights, entitlements and opportunities of an individual.*	□	□	☑
Systematic monitoring or tracking of individuals? *For example, the introduction or enhancement of a surveillance system, the monitoring of communications, tracking an individual's geolocation or behaviour.*	□	□	☑
Collecting personal information without notification to, or consent of, the individual? *This might include collecting personal information about an individual from a third party without the individual's knowledge or consent. It might also include collecting personal information compulsorily under an existing, or proposed, legislative authority.*	□	□	☑
Data matching (linking unconnected personal information)? *For example, a new data matching program combining, comparing or matching personal information obtained from multiple sources.*	□	□	☑
Any other relevant factors that may have a significant impact on the privacy of individuals?	□	□	☑

Part 3: Decision & declaration

If you have answered 'Yes' or 'Potentially' to any of the questions in Part 2, a PIA should be completed. If you are uncertain as to whether you have considered all relevant risks, you are strongly encouraged to seek support from the Privacy Officer to ensure your assessment is thorough and complete. If still unsure, err on the side of caution and conduct a PIA.

Based on your answers above, is a PIA required?

□ **Yes** Yes, there are (or potentially are) high privacy risk elements to this project.

☑ **No** No, a PIA is not necessary. The project does not carry any high privacy risks.

Business owner sign-off

Position	Date
A/g Director, Cyber Security	16/03/2021

Privacy Officer sign-off

Position	Date
Director, Governance	16/03/2021