

High-Level Cyber Security Risk Assessment Questionnaire

Provider Registration and International Student Management System (PRISMS)

## Purpose

The Department of Education (the department) are responsible for ensuring that any organisation it contracts to deliver services on their behalf, have adequate security processes and controls in place. This includes any processes to protect sensitive and government or participant data accessed, generated, held, or managed, in their supply chain. The department will be working closely with the Department of Employment and Workplace Relations (DEWR) to strengthen the security of the utilised IT systems.

The intent of this cyber security questionnaire is to develop a base level of understanding of the security posture for each vendor or provider. This questionnaire attempts to determine how an organisation will store and manage data. As such, responses should be collated from staff with the relevant knowledge within the organisation.

## How to complete this questionnaire

This questionnaire covers a broad range of cyber security topics including governance, personnel processes, use of information, and Information Communications Technology (ICT) services and processes to identify and report a cyber security breach. While multiple staff in your organisation may be required to answer various sections, the department requests the responsible authority, i.e. CEO, sign the declaration.

If you are a vendor or provider that is part of a consortium or a group, each organisation must respond to this questionnaire independently.

## Minimum evidence requirements

* All questions must be answered.
* Where required, please provide further information to support your answer.
* Where you have answered ‘yes’ to a question, evidence must be available at the department’s request.
* Where you have answered ‘no’ or ‘unsure’, please provide a brief explanation as to why this is the case.
* A high-level cyber security risk assessment will be made on the information provided in this questionnaire. Please ensure your responses are true and correct to the best of your knowledge.

## What’s next?

* Your submission will be reviewed and evidence to support your answers may be requested to help the department understand the security posture of your organisation.

Completing this questionnaire is the beginning of meeting Right Fit For Risk (RFFR) requirements. It is recommended that vendors or providers understand the RFFR obligations they may be required to achieve should the department require this. Further information is available on the DEWR website - [Right Fit For Risk Cyber Security Accreditation - Department of Employment and Workplace Relations, Australian Government (dewr.gov.au)](https://www.dewr.gov.au/right-fit-risk-cyber-security-accreditation).

# High-Level Cyber Security Risk Assessment Questionnaire Provider Registration and International Student Management System (PRISMS)

|  |  |
| --- | --- |
| **Question** | **Answer** |
| Entity legal/trading name |  |
| Registered ABN |  |
| Registered address |  |
| Education provider or Software vendor | Education provider / Software vendor |

|  |
| --- |
| 1. **Your Organisation**
 |
| **1.1a.** **Vendor:** How many CRICOS providers do you intend to service through the PRISMS API? |  |
| **1.1b. CRICOS Provider:** How many Confirmations of Enrolment do you intend to create through the PRISMS API? | [ ]  Under 200 Confirmations of Enrolment/year [ ]  200 - 2000 Confirmations of Enrolment/year [ ]  Over 2,000 Confirmations of Enrolment/year |
| **1.2.** How many employees do you currently have in your organisation as a whole? |  |
| **1.3.** How many employees will be involved in delivering services under the PRISMS API? |  |
| **1.4.** How many physical business sites will deliver services under the PRISMS API? |  |
| 1. **Your Information Security Management System (ISMS)**
 |
| **2.1.** Does your organisation currently hold any ICT Security Accreditation? *If so, please provide the type, date, and currency of the accreditation.* |  |
| **2.2.** Has your organisation participated in Right Fit For Risk in the past? *If so, please detail each milestone and when they were completed, along with the date if accreditation was granted.* |  |
| **2.3.** Please describe your experience in managing an environment for the collecting, storing and processing of information classified at the OFFICIAL: Sensitive level.*A description of Official: Sensitive information is available at:* [*https://www.protectivesecurity.gov.au/publications-library/policy-8-classification-system*](https://www.protectivesecurity.gov.au/publications-library/policy-8-classification-system)*.*  |  |
| **2.4.** Has your organisation ever performed a Privacy Impact Assessment covering your general operations and IT systems to address your management of personal information?*If so, please detail the recommendations and progress towards implementing those recommendations.****Note:*** *You are not required to undertake a Privacy Impact Assessment at this stage. However, should the department require you to formally commence the RFFR process, you will be required to undertake a Privacy Impact Assessment covering your general operations and IT systems as part of meeting RFFR requirements, including confirmation that all the recommendations in the Privacy Impact Assessment have been addressed.**See guide:* [*https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/*](https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/)*.* |  |
| **2.5.** Do you have an Incident Response Plan or Data Breach Response plan? *If so, have these plans been tested?* |  |
| **2.6.** Have you experienced any reportable cyber security incidents or notifiable data breaches within the past 3 years?*ASD’s ACSC Reportable Cyber Security Incidents:* [*https://www.cyber.gov.au/report-and-recover/report*](https://www.cyber.gov.au/report-and-recover/report)*.**Notifiable Data Breach:* [*https://www.oaic.gov.au/privacy/notifiable-data-breaches*](https://www.oaic.gov.au/privacy/notifiable-data-breaches)*.* |  |
| **2.7.** What other policies and procedures does your organisation have regarding access to, and the handling of information in your IT systems. |  |
| 1. **Data Sovereignty**
 |
| **3.1.** Please describe your understanding of your obligations regarding Data Sovereignty that are necessary as part of the PRISMS API access. |  |
| **3.2.** Are any of your ICT systems hosted offshore? *If yes, further information is required in question 3.4, 3.5 and Section 6 below.* |  |
| **3.3.** Are any of your existing ICT systems accessed from offshore locations? *This may include staff working remotely, or system administration access.* ***If yes, please provide further information within question 3.4, 3.5 and Section 6 below.*** |  |
| **3.4** Do these systems collect, store, or process departmental data or participants personal or sensitive information? |  |
| **3.5** Do you have the capacity or capability to migrate these ICT systems to an equivalent Australian based solution? |  |
| 1. **Your Personnel Onboarding**
 |
| **4.1** Does your organisation have a matured and documented personnel onboarding processes? *E.g., conducting background checks such as Working with Children, Police check, Referee check, CV validation etc.* |  |
| **4.2** Do you provide your staff with information security awareness training and privacy awareness training that they must complete prior to having access to your systems? |  |

## Essential Eight strategies to mitigate cyber security incidents

The Australian Signals Directorate (ASD) has developed prioritised mitigation strategies, in the form of the ***Strategies to Mitigate Cyber Security Incidents***, to help organisations protect themselves against cyber threats. The most effective of these mitigation strategies are the Essential Eight. When implementing the Essential Eight, organisations should first identify a target maturity level that is suitable for their environment and the value of the data held.

Organisations should then progressively implement each maturity level until that target is achieved. As the mitigation strategies that constitute the Essential Eight have been designed to complement each other, and to provide coverage of various cyber threats, organisations should plan their implementation to achieve the same maturity level across all eight mitigation strategies before moving onto higher maturity levels.

The department expects that organisations achieve Maturity Level 1 (ML1) as an initial baseline. Further information on Maturity Levels is available at <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model>.

|  |
| --- |
| 1. **Your ISMS Essential Eight Maturity**
 |
| **Essential Eight Implementation****Please ensure the below section is completed by your technical specialist.****For the full list of ML1 control requirements please refer to:** <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model-ism-mapping>.**Essential Eight Implementation Status Definitions (per the department)****Not implemented:** The solution, if any, is not effective.**Partially implemented:** The solution is not fully effective or is only implemented on some relevant assets.**Fully implemented:** The solution effectively meets the control objective.**Note:** In some cases, you may have effective alternate or compensating controls. If so, please describe these in the relevant sections below. |
| **5.1 Essential Eight*****Briefly describe your organisation's approach to implementation of the Essential Eight strategies.***  |  |
| **5.2 Patch Applications***December 2023 ISM Control Ref:**1807, 1808, 1698, 1699, 1876, 1690, 1691, 1905, 1704.* | [ ]  Not implemented[ ]  Partially implemented[ ]  Fully implemented, all controls achieve ML1 at a minimumDetail of current implementation: |

|  |  |
| --- | --- |
| **5.3 Patch Operating Systems***December 2023 ISM Control Ref:**1807, 1808, 1701, 1702, 1877, 1694, 1695, 1501.* | [ ]  Not implemented[ ]  Partially implemented[ ]  Fully implemented, all controls achieve ML1 at a minimumDetail of current implementation: |
| **5.4 Multi-Factor Authentication***December 2023 ISM Control Ref:**1504, 1679, 1680, 1892, 1893, 1681, 1401.* | [ ]  Not implemented[ ]  Partially implemented[ ]  Fully implemented, all controls achieve ML1 at a minimumDetail of current implementation: |
| **5.5 Restrict Administrative Privileges***December 2023 ISM Control Ref:**1507, 0445, 1175, 1883, 1380, 1688, 1689.* | [ ]  Not implemented[ ]  Partially implemented[ ]  Fully implemented, all controls achieve ML1 at a minimumDetail of current implementation: |
| **5.6 Application Control***December 2023 ISM Control Ref:**0843, 1870, 1657.* | [ ]  Not implemented[ ]  Partially implemented[ ]  Fully implemented, all controls achieve ML1 at a minimumDetail of current implementation: |
| **5.7 Restrict Microsoft Office Macros***December 2023 ISM Control Ref:**1671, 1488, 1672, 1489.* | [ ]  Not implemented[ ]  Partially implemented[ ]  Fully implemented, all controls achieve ML1 at a minimumDetail of current implementation: |
| **5.8 User Application Hardening***December 2023 ISM Control Ref:**1654, 1485, 1486, 1585.*  | [ ]  Not implemented[ ]  Partially implemented[ ]  Fully implemented, all controls achieve ML1 at a minimumDetail of current implementation: |
| **5.9 Regular Backups***December 2023 ISM Control Ref:**1511, 1810, 1811, 1515, 1812, 1814.* | [ ]  Not implemented[ ]  Partially implemented[ ]  Fully Implemented, all controls achieve ML1 at a minimumDetail of current implementation: |

|  |
| --- |
| 1. Your ICT Environment and Third-Party Services
 |
| **Please ensure the below section is completed by your technical specialist.** |
| 6.1 On-Premise ICT InfrastructureDescribe any on-premise ICT infrastructure used within your environment. This includes any physical/virtual servers (including email hosting and data storage capabilities), endpoints and networking devices. |  |
| 6.2 Cloud ServicesDescribe all ICT cloud services used within your environment. This includes IaaS, SaaS and PaaS.For example: ‘We consume Microsoft 365 for business hosted within the Australian East region, as well as an AWS S3 storage solution hosted in the Sydney region.’.Note: Australian onshore storage is required under the RFFR approach. |  |
| 6.3 TPES – Third Party Employment and Skills SystemsDescribe all currently used client management applications purchased from, and managed by, a vendor to support service delivery. Examples of current DEWR RFFR Accredited TPES Systems are available on the DEWR Website: [*https://www.dewr.gov.au/right-fit-risk-cyber-security-accreditation/accredited-third-party-employment-and-skills-tpes-systems*](https://www.dewr.gov.au/right-fit-risk-cyber-security-accreditation/accredited-third-party-employment-and-skills-tpes-systems). |  |
| **6.4 MSP** – **Managed Services Provider**Describe all currently engaged managed service providers that manage or deliver any part of your ICT environment, infrastructure, system administration, document destruction, or other, on your behalf. |  |

|  |
| --- |
| **Please provide any additional comments that are not addressed in the questionnaire:** |
|  |
|  |
|  |

# CEO declaration

I, <name, position>, on behalf of <organisation> declare that the information provided within this questionnaire is true and correct.

[ ]  I agree that the department will be notified of any changes in relation to the information supplied in this questionnaire, should they occur.

[ ]  I agree to implement or strengthen my organisation’s information security posture as reasonably required by the department.

|  |  |  |
| --- | --- | --- |
| **Signatory / CEO / CRICOS Principal Executive Officer** | **Name** |  |
| **Signature** |  |
| **Date** |  |
| **Email address** |  |
| **Phone number** |  |
| **Position** |  |

|  |  |  |
| --- | --- | --- |
| **Witness** | **Name** |  |
| **Signature** |  |
| **Date** |  |
| **Email address** |  |
| **Phone number** |  |
| **Position** |  |

Please submit your completed questionnaire via email to: prismsapi@education.gov.au.