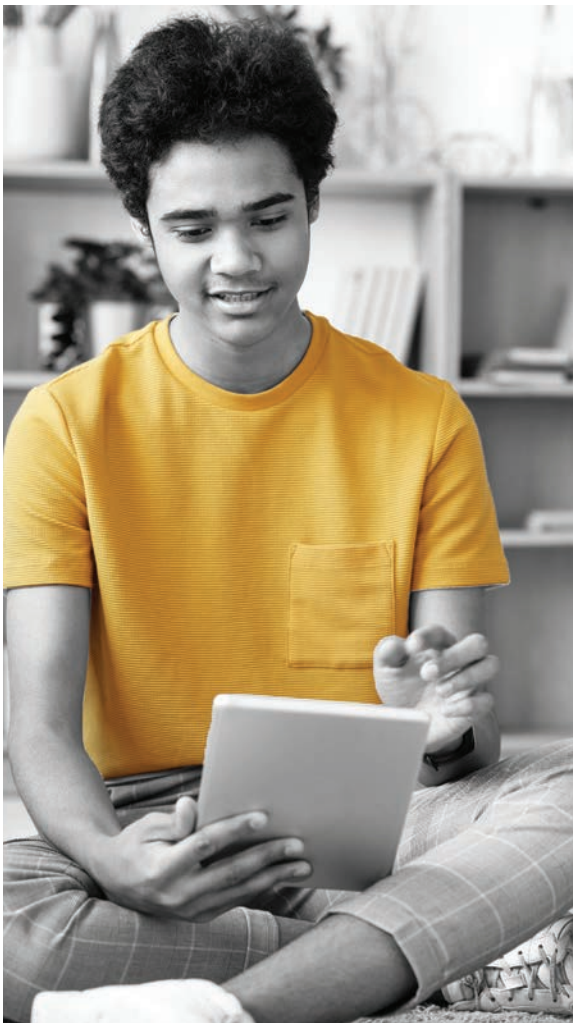
GESS

Global Education Security Standard

Controls for Education Services



Global Education Security Standard (GESS) is a matrix/crosswalk of all existing security frameworks along with the core set of controls applicable to PK-20 data.

With the range of technical, functional, cyber security, data protection, privacy and other requirements, it is increasingly laborious to demonstrate compliance during procurement exercises.

With the growing number of security standards and frameworks, there is a significant amount of crossover, and much of it not in a language that allows for consideration of educational or operational needs of educational institutions. GESS streamlines this process by identifying and cross walking security controls that are applicable in Educational Technology products.

Building on the success of the ST4S assessments across Australia and New Zealand, the Student Data Privacy Consortium has brought together a working group of educational departments, leading vendors and academics to develop a Global Education Security Standard, to provide a common grounding baseline for all, as well as regional requirements.

More About GESS

GESS is an internationally agreed upon set of security controls pulled from major cyber security frameworks that are most applicable to the PK20 education ecosystem.

By joining the GESS subscribers you will be aiding the movement of the EdTech industry towards one common set of security controls to apply across many jurisdictions, thus avoiding the need to prove certification in multiple frameworks PK20 schools and districts are adopting the GESS set of controls as the expected security measures to be in place to protect all student data.

In the US the next version of the National Data Privacy Agreement will include the GESS as an approved and accepted control framework. In Australia & New Zealand the preexisting ST4S controls are embedded within GESS.

GESS will streamline both the providers' ability to implement required security controls while at the same time meeting school expectations all with one common set of controls.

Release: 1.2
Date of this version: February 28, 2024
Author: GESS Project Team

GESS Disclaimer

The Global Education Security Standard (“GESS”) is an identified set of security controls taken from relevant standards and legislation intended to be employed by marketplace providers in the Educational Technology field. Adherence to the usage conditions outlined in the GESS does not guarantee information security and user safety while using the online service. Users should always exercise caution when using online services and contact their local support team for assistance if required.

THE GLOBAL EDUCATION SECURITY STANDARD IS PROVIDED “AS IS.” A4L MAKES NO WARRANTY OF ANY KIND, EXPRESS, IMPLIED, IN FACT OR ARISING BY OPERATION OF LAW, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT AND DATA ACCURACY. A4L NEITHER REPRESENTS NOR WARRANTS THAT THE OPERATION OF THE GESS PORTAL SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT ANY DEFECTS WILL BE CORRECTED. A4L DOES NOT WARRANT OR MAKE ANY REPRESENTATIONS REGARDING THE USE OF THE SOFTWARE OR THE RESULTS THEREOF, INCLUDING BUT NOT LIMITED TO THE CORRECTNESS, ACCURACY, RELIABILITY, OR USEFULNESS OF GESS.

You are solely responsible for determining the appropriateness of using and distributing the GESS and you assume all risks associated with its use, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and the unavailability or interruption of operation. This GESS is not intended to be used in any situation where a failure could cause risk of injury or damage to property.

830-100/6785757.1

Commonly Used Terms

The following are commonly used terms throughout this document:

Your organisation: The organisation responsible for producing the product being evaluated (as a software producer).

Vendor: The organisation responsible for producing the product being evaluated (as a commercial entity)

Sub-contractor: Other organisations, engaged by your organization in the process of producing or supporting the product being evaluated. Also referred to as sub-processors.

Independent third party: A supplier of goods and services other than your organisation or its sub-contractors.

IT: Information technology

ICT: Information and communications technology (i.e. telephones and audiovisual devices, as well as computers and computer infrastructure)

Country of assessment: The country in which the assessment is being undertaken, on behalf of school authorities in that country

Data Controller: The organisation(s) who decide the purpose and means of processing

Data Processor: Organisation or body which processes personal data on behalf of the data controller.

Personal Data: Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Pseudonymisation: The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person

Anonymous data: Information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable, and cannot be re-identified.

Data De-identification: A Visual Guide to Practical Data De-Identification (fpf.org) gives a good overview of the different stages. Will look for suitable terms for this and anonymisation

Anonymisation: As above

Transfer: The movement of personal data for processing or the intention of processing, from the customer to your organisation/the vendor, or from your organisation

Data Processing Agreement / Privacy Policy: A clear agreement between Your Organisation / the Vendor and the customer, establishing what personal data is processed and other statutory information as set out by the customer's region (e.g. location, security information, retention, transfers)

1 Assessment Criteria

Criteria for assessing a software product for security and other relevant concerns.

1.1 Criteria | Company & product detail

Contact and related details of the vendor.

#	Question	Tier	Notes
C0	For which countries are you submitting a GESS survey response?	1 & 2	Response options: 1. All countries (USA, Australia, New Zealand) 2. Australia only 3. New Zealand only 4. USA only
C1	Vendor name	1 & 2	Informational
C2A	Vendor ABN	1 & 2	Informational (AU submissions)
C2B	Vendor NZBN	1 & 2	Informational (NZ submissions)
C2C	Vendor US corporate number CRN	1 & 2	Informational (USA submissions)
C2D	Vendor UK registration number	1 & 2	Informational (UK submissions)
C3A	Registered Australian address of vendor	1 & 2	Informational (AU submissions)
C3B	Registered New Zealand address of vendor	1 & 2	Informational (NZ submissions)
C3C	Registered USA address of vendor	1 & 2	Informational (USA submissions)
C4A	Country in which the company is registered for Australian customers	1 & 2	Informational (AU submissions)
C4B	Country in which the company is registered for New Zealand customers	1 & 2	Informational (NZ submissions)
C4C	Country in which the company is registered for USA customers	1 & 2	Informational (USA submissions)
C5A	For Australian customers: Preferred vendor contact name Preferred vendor contact email Preferred vendor contact phone number	1 & 2	Informational (AU submissions)
C5B	For New Zealand customers: Preferred vendor contact name Preferred vendor contact email Preferred vendor contact phone number	1 & 2	Informational (NZ submissions)
C5C	For USA customers: Preferred vendor contact name Preferred vendor contact email Preferred vendor contact phone number	1 & 2	Informational (USA submissions)

1.2 Criteria | Security

Criteria relevant to the assessment of the software product for security, as distinct from privacy or interoperability.

Standard references are taken from:

- NIST 800-171 Revision 2: https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
- the Australian Government Information Security Manual June 2022 (AUISM): https://www.cyber.gov.au/ism; and
- the New Zealand Information Security Manual v3.6 (NZISM): https://www.nzism.gcsb.govt.nz/
- the Australian Privacy Principles (APP): https://www.oaic.gov.au/privacy/australian-privacy-principles/read-the-australian-privacy-principles/.
- the New Zealand Privacy Principles (NZPP): https://privacy.org.nz
- Critical Security Controls (CIS controls) v8: https://www.cisecurity.org/controls/v8

In the response options column:

- the minimum acceptable response is in bold;
- the relevant assessment tier is written in brackets as a prefix to the minimum acceptable response, where "T1" means Tier 1, "T2" means Tier 2, and "T1, T2" means both Tier 1 and Tier 2. Where a country code or country/state is also provided (e.g., for control H6 – AU T1, AU T2), this indicates that this response is a minimum for that particular country only or particular country & specific state.
- a hash # (also known as an octothorpe) indicates that the question is of high importance. Failure to meet the minimum acceptable response will result in a "Non-compliant" assessment outcome.

1.2.1 Security | Product function

Overall details of the product being evaluated, and of the basic functionality offered that relate to product security.

#	Question	Tier	Response Options	Standard
P1	Name of service	All		
P2A	Version of service If no published version number, use date of version.	All		
P2B	Is the service free or paid?	All	A. Free B. Paid C. Both/Hybrid	
P2C	For paid services, URL of pricing page	All		
P2D	Are you the product or service's original developer, a re-seller or 'other'?	All	A. Original developer B. Reseller C. Other (please specify)	
P2E	Do you warrant that you have the legal authority to submit this product or service for a GESS assessment?	All		
P3A	URL of service for customers in the country of assessment	All	A. No# B. Yes (T1, T2)	

1.2.1 Security | Product function (continued...)

#	Question	Tier	Response Options	Standard
P3A	URL of service for customers in the country of assessment	All		
P3B	URL of service for neighboring countries that are routinely linked commercially (e.g. US/CA, AU/NZ)	All		
P3C	URL of service for customers in the home country of the vendor	All		
P3D	URL for International/Other customers	All		
P4A	URL of Terms of Service/use for Australian customers	All		
P4B	URL of Terms of Service/use for New Zealand customers	All		
P4C	URL of Terms of Service/use for USA customers	All		
P5	Purpose of the service?	1 & 2		
P6	In what jurisdiction would disputes, regarding usage of the service, be handled? (e.g., Washington USA, Victoria Australia, New Zealand)	1		
P7	Does your organisation have a current insurance policy of at least $1M with claims for data breach/loss?	All	A. Yes - current policy with coverage of at least $1 million (T1) B. Yes - current policy but coverage is less than $1 million C. No current policy	UKCE A3.1 - 3.4
P8	Is this service dependent on another IT service to function according to its intended purpose? (e.g., does this service have YouTube embedded or rely on Facebook logins?) For example, does the service utilize any third party/outsourced: • plug ins • browser extensions • hosting services • video streaming services (e.g., YouTube, Vimeo) • image hosting services • data processing service • publishing services etc.		A. Yes, please specify B. No	NZISM 12.7, UKCE A2.9

1.2.1 Security | Product function (continued...)

#	Question	Tier	Response Options	Standard
P9	When using the service for its intended purpose, what, if any, of the data types below would reasonably be captured, stored, or processed by the service? Select all that apply. *Sensitive information is a type of personal information that is given extra protection and must be treated with additional care. If in doubt, select this option. Sensitive information may include:* • *Protection details (i.e., whether the user is under a protection order and/or the details of the order)* • *Legal custodian arrangements and court orders* • *Out of home care status* • *Records of behavior incidents/discipline, behavioral observations/notes* • *Consent (e.g., collection and/or recording of consent)* • *Student absence details (i.e., records of attendance and reason for absence)* • *Records of contact (e.g., between parents, teacher, school, and/or student) and other agencies* • *Student/Learning support service information and support arrangements* • *Enrollment support records (sensitive case, complex case, adjustments, student plan, developmental map, transportation, Individual Education Plans, Oranga Tamariki 'All about Me' plan)*	All	• Protection order details (student) • Legal custodial arrangements (student) • Informal custodial arrangements • Legal status (criminal convictions, protection orders, police checks results etc) • Out of home care status (student) • Records of behavior incidents (student) • Records of incidents • Behavioral observations/notes (student) • Records of contact or interview (student) • Sensitive social, emotional or mental health and well-being information (staff, student, parent) • Support arrangements (student) • Professional case notes (student) • Reason for absence (student) • Commonwealth Unique Student Identifier (AU) or National Student Number (NZ) • Health and medical details, including mental health diagnoses (staff, student, parent) • Financial information (staff, student, parent, organisation) • Identification documentation (staff, student, parent) • Digital signature (staff, student, parent) • Government related Identifiers (e.g., state or federal government assigned identifiers) • Official records • Racial or ethnic origin • Religious beliefs or affiliations • Sexual orientation or practices • Biometric information (e.g., eye/retinal/facial imagery, fingerprints, biometric templates) • Location tracking data (Information about the ongoing geographic positions of individuals or devices derived from GPS or other network sources. Examples include: Current position in time and retained point in time, ongoing positions of individuals, cellular network connection tracking, BLE (Bluetooth Light Energy) beacons communication) • Use of social services (Work & Income, ACC, CYPS, Women's refuge etc) • None of the above (T2)	NZ PSR – INFOSEC1

1.2.1 Security | Product function (continued...)

#	Question	Tier	Response Options	Standard
P10	Select the functionality available within the service. Select all that apply.	All	• Online meetings, video or audio conferencing, livestreaming (T1) • Activity and Permissions Management (e.g. consent slips) (T1) • Financial management or payment processing systems (T1) • Enrollment management (T1) • Student information, student management system, school administration or student administration system (T1) • Customer relationship management (T1) • Ticketing system - Service Management, Helpdesk (T1) • Learning management system (T1) • Electronic document and records management systems (T1) • File hosting and synchronization (T1) • Remote access (T1) • Data collection tools (non-curriculum) (T1) • Photo, image, video or audio storage, sharing and backup services (T1) • Two-way communication tools (T1) • Data aggregation, Data broker, Data hub, Data distribution hub (T1) • Software and cloud developer tools (T1) • Collaboration and sharing (T2) • One-way communication tools (T2) • Career education, planning and guidance (T2) • Vocational training providers and courses, industry/employment registers, work placements (T2) • Learning activities, assessments and games (T2) • Content creation, presentation tools and publishing (T2) • Educational resources and content libraries (T2) • File download, including executables (T2) • Library Management (T2) • Visitor Management (T2) • Event management, bookings, online ordering or fundraising (T2) • Administrative support services and tools (T2) • None of the above (T2)	

1.2.1 Security | Product function (continued...)

#	Question	Tier	Response Options	Standard
P11	Does the service contain, display, or promote the following via any means (social media or news feed, direct advertising, pop-ups): • Products/services: alcohol, controlled or banned substances, gambling, tobacco products, firearms and firearm clubs, adult products and pornography. • Categories of information which may be deemed offensive by a reasonable member of the school community (e.g., racist, sexist, pornographic content etc.)	All	A. Yes (please specify) B. No (T2)	
P12	With regards to any third-party providers, subcontractors or sub-processors that make up the solution, or provide service to you, does your organisation: • have an inventory of all third-party service providers, subcontractors or sub-processors; • regularly assess and manage the risks associated with these parties; • have contractual agreements in place to ensure these parties adhere to your information security and privacy policies; • ensure that the contractual agreements include notification of the transfer or termination of any personnel authorized to use your organisation's systems; • monitor these parties for compliance; and • have defined and documented roles and responsibilities with regards to these parties, including oversight of compliance • have a classification system for these parties; and • have a designated internal organisation contact for each party?	1	A. No B. Yes - for some third-party providers and subcontractors C. Yes - for all third party-providers and subcontractors (T1) D. NA - solution does not use third party providers or subcontractors (T1)	NZ PSR - GOV5 NZISM 12.7 NZPP-5 NZPP-11 NIST 800-53 PS-7 NIST 800-53 SA-9 CIS 15.1 UKCE A2.9

1.2.1 Security | Product function (continued...)

#	Question	Tier	Response Options	Standard
P13	For the service being assessed, what is the deployment architecture used for customers?	All	A. Hosted in customer environment B. Hosted in environment owned or managed by your organisation C. Both hosted in customer environment and an environment owned or managed by your organisation	
P14	Is the service compliant with the WCAG 2.1 Accessibility guidelines as per https://www.w3.org/WAI/standards-guidelines/wcag/	All	A. No B. Yes – all components meet WCAG 2.1 AAA C. Yes – all components meet minimum of WCAG 2.1 AA D. Yes – all components meet minimum WCAG 2.1 A (T1, T2)	
P15	Does your organisation seek to absolve indemnity from any legal liabilities with regards to the operation of the service?	1 & 2	A. No (T1, T2) B. Yes, outlined in publicly available terms of service or other public document or public location (please specify and provide link) (T1, T2) C. Yes, outlined in a non-publicly available document or non-publicly available location and not actively provided to customers (T1, T2) D. Yes, outlined in a document the vendor proactively provides to all customers prior to contract phase (T1, T2)	NZ Govt Web Standards

1.2.2 Security | Hosting and Location

Evaluation of how the product is hosted online.

#	Question	Tier	Response Options	Standard
H1	Select the option which best describes where user data or any related data (e.g., metadata, logs, user content) is stored or processed across all components of the service, including live solution, backup, disaster recovery, test environment, and development environments.	1 & 2	A. Entirely in a country nominated by the customer, in accordance with local legislation, and with no transfer of data outside the nominated country (specify supported countries for the country of assessment) (T1, T2) B. Entirely by a single vendor and its subcontractors, in a single country nominated by the vendor, and with no transfer of data outside the nominated country (specify country) C. Entirely by a single vendor and its subcontractors, in multiple vendor nominated countries: • Live solution (please specify country/s) • Other components (backup, etc) (please specify country/s) D. By multiple vendors and their subcontractors, in one or more vendor nominated countries: • Live solution (please specify vendor or subcontractor, applicable personal data categories, country/s) • Other components (backup, etc) (please specify vendor or subcontractor, applicable personal data categories, country/s)	AUISM Security Control: 1452 Revision 3 NZISM 22.1.22 NZISM 12.7 NZPP-11
H2	From what countries do vendor staff, including support, administration, development and testing, and external contractors or associates, access user data and any related data (e.g., metadata, logs) collected or used by the service (including backups and recovery)?	1 & 2	A. Entirely from a single customer country (please specify) B. Entirely from a single vendor nominated country (please specify) C. From multiple countries (please specify country/s)	AUISM Security Control: 0975 Revision 7 NZISM 22.1.22 NZISM 12.7 UKCE A2.1 UKCE A2.2 UKCE A2.3
H3	Retired (2022)			

1.2.2 Security | Hosting and Location (continued...)

#	Question	Tier	Response Options	Standard
H4	At a minimum, are the following physical access controls in place at the locations where data is stored: • No public access; • Visitor access only for visitors with a need to know and with a close escort; • Restricted access for authorized personnel with appropriate security clearance; • Physical controls on the facility and its support infrastructure (e.g. locked wiring closets); • Single factor authentication for access control using a secure swipe card, biometrics or coded access; • Security alarm system; • Physical surveillance (e.g. video cameras); • Logging of any access to locations where data is stored or processed by any person with reporting of any identified anomalies; and • Logging of any delivery and removal of physical system components.	1	A. Yes – all of the above (T1) B. Yes – some of the above C. No – none of the above	AUISM Security Control: 1296 NZISM 8.1 NIST 800-171 3.10.1 NIST 800-171 3.10.2 NIST 800-171 3.10.3 NIST 800-171 3.10.4 (DESIRABLE) NIST 800-171 3.10.5 NIST 800-53 PE-6(1) NIST 800-53 PE-8 NIST 800-53 PE-16 UKCE A2.4 UKCE A4.2
H5	Are customers notified of any relocation or expansion (i.e. change of country) of: • the cloud infrastructure, including system components, user data and related data; and • any person (vendor or cloud infrastructure staff, external contractors or associates) with access to unencrypted customer data or any person with a means of accessing or extracting unencrypted data (e.g., those with access to encryption keys and encrypted customer data), • prior to relocation?	1 & 2	A. No (#T1, #T2) B. Yes (specify average notification lead time) (T1, T2)	AUISM Security Control: 1578 Revision 0 NZISM 22.1.22 NZISM 12.7

1.2.2 Security | Hosting and Location (continued...)

#	Question	Tier	Response Options	Standard
H6	If the service includes outsourced cloud-based services, are those cloud-based services IRAP assessed? See https://www.cyber.gov.au/irap for information about IRAP assessment.	1 & 2	A. No or unknown B. Yes – some outsourced cloud-based services are IRAP assessed C. Yes – all outsourced cloud-based services are IRAP assessed (AU T1, AU T2) D. Not applicable – service does not include outsourced cloud-based services (AU T1, AU T2)	AUISM Security Control: 1570 Revision 0 UKCE A2.9

1.2.3 Security | Technical

Criteria around the technical implementation of security in the product.

#	Question	Tier	Response Options	Standard
S1	What are the minimum encryption algorithms applied to protect all data in transit over networks, including encryption of data that is communicated between the user, web applications and system components (e.g., database systems)?	1 & 2	A. No encryption (#T1, #T2) B. Encryption: DES, RC4, 3DES using three distinct keys; (#T1, #T2) Hashing: Message Digest (MD to MD6), RIPEMD-128 or above, SHA-0, SHA-1; Digital Signatures: DSA (1024) or RSA (1024); Key Exchange: DH (1024) or RSA (1024); Protocol: TLS1.1 or below C. Encryption: AES 128 or above; Hashing: SHA-224 or above Digital Signatures: DSA (2048) FIPS 186-4, ECDSA (224+) preferably using NIST P-384 curve or RSA (1024+); Key Exchange: DH (2048+), ECDH (256+) preferably using NIST P-384 curve and/or RSA (2048+); Protocol: TLS 1.2 or above only(T2) D. Encryption: AES 192 GCM/CCM, CHACHA20 POLY 1305 or above only (AES 256 GCM/CCM recommended); Hashing: SHA-256 or above only (SHA-384 recommended); Digital Signatures: DSA (2048+) FIPS 186-4, ECDSA (224+) using NIST P-384 curve or RSA (2048+); Key Exchange: DH (3072+), ECDH (256+) using NIST P-384 curve and/or RSA (3072+); Protocol: TLS 1.2 or above only (TLS 1.3 recommended) (T1)	AUISM Security Control: 1139, revision 5; ISM Security Control: 0471, revision 6; AUISM Security Control: 1277, revision 2. AUISM Security Control: 0994. NZISM 17.2 NZISM 17.3 NIST 800-171 3.13.8 NIST 800-171 3.13.11 NIST 800-171 3.13.15

1.2.3 Security | Technical (continued...)

#	Question	Tier	Response Options	Standard
S2	What are the minimum encryption algorithms applied to protect data at rest, including backups, data storage and auditable logs?	1 & 2	A. Yes (T1, T2) B. No	NIST 800-171 3.13.4
S2a	Does the service prevent unauthorized and unintended information transfer via unencrypted shared system resources, such as caches and hard disks? If customer data is uploaded to the service using a mechanism such as encrypted USB, SFTP, Secure API, etc., what are the minimum encryption methodologies applied?	1 & 2	A. No encryption (#T1, #T2) B. Encryption: DES, RC4, 3DES using three distinct keys; (#T1, #T2) Hashing: Message Digest (MD to MD6), RIPEMD-128 or above, Secure Hash Function (SHA-0, SHA-1); Digital Signatures: DSA (1024) RSA (1024); Key Exchange: DH (1024), RSA (1024); Protocol: TLS 1.1 or below C. Encryption: AES 128 or above; Hashing: SHA-224 or above Digital Signatures: DSA (2048) FIPS 186-4, ECDSA (224+) preferably using NIST P-384 curve or RSA (1024+); Key Exchange: DH (2048+), ECDH (256+) preferably using NIST P-384 curve and/or RSA (2048+); Protocol: TLS 1.2 or above only(T2) D. Encryption: AES 192 GCM/CCM, CHACHA20 POLY 1305 or above only (AES 256 GCM/CCM recommended); Hashing: SHA-256 or above only (SHA-384 recommended); Digital Signatures: DSA (2048+) FIPS 186-4, ECDSA (224+) using NIST P-384 curve or RSA (2048+); Key Exchange: DH (3072+), ECDH (256+) using NIST P-384 curve and/or RSA (3072+); Protocol: TLS 1.2 or above only (TLS 1.3 recommended) (T1) E. N/A - Customer data is not uploaded to the service	AUISM Security Control: 1139, revision 5; AUISM Security Control: 0471, revision 6; AUISM Security Control: 0472, revision 6; AUSIM Security Control 1759, revision 0; AUSIM Security Control 0474, revision 6; AUSIM Security Control 1761, revision 0; NZISM 17.2 NZISM 17.3 NIST 800-171 3.13.8 NIST 800-171 3.13.11

1.2.3 Security | Technical (continued...)

#	Question	Tier	Response Options	Standard
S3	If customer data is uploaded to the service using a mechanism such as encrypted USB, SFTP, Secure API, etc., what are the minimum encryption methodologies applied?	1 & 2	A. No encryption (#T1, #T2) B. Encryption: DES, RC4, 3DES using three distinct keys; (#T1, #T2) Hashing: Message Digest (MD to MD6), RIPEMD-128 or above, Secure Hash Function (SHA-0, SHA-1); Digital Signatures: DSA (1024) RSA (1024); Key Exchange: DH (1024), RSA (1024); Protocol: TLS 1.1 or below C. Encryption: AES 128 or above; Hashing: SHA-224 or above Digital Signatures: DSA (2048) FIPS 186-4, ECDSA (224+) preferably using NIST P-384 curve or RSA (1024+); Key Exchange: DH (2048+), ECDH (256+) preferably using NIST P-384 curve and/or RSA (2048+); Protocol: TLS 1.2 or above only(T2) D. Encryption: AES 192 GCM/CCM, CHACHA20 POLY 1305 or above only (AES 256 GCM/CCM recommended); Hashing: SHA-256 or above only (SHA-384 recommended); Digital Signatures: DSA (2048+) FIPS 186-4, ECDSA (224+) using NIST P-384 curve or RSA (2048+); Key Exchange: DH (3072+), ECDH (256+) using NIST P-384 curve and/or RSA (3072+); Protocol: TLS 1.2 or above only (TLS 1.3 recommended) (T1) E. N/A - Customer data is not uploaded to the service	AUISM Security Control: 1139, revision 5; AUISM Security Control: 0471, revision 6; AUISM Security Control: 0472, revision 6; AUSIM Security Control 1759, revision 0; AUSIM Security Control 0474, revision 6; AUSIM Security Control 1761, revision 0; NZISM 17.2 NZISM 17.3 NIST 800-171 3.13.8 NIST 800-171 3.13.11
S4	If multi-tenancy is used (i.e. system components are shared between multiple customers), are partitioning controls implemented to securely segregate one customer's data from another customer's data? E.g. • Assign a unique customer ID when same table is used to store multiple customers' data • Use separate table or database for each customer • Use a separate instance, environment or VPC	1 & 2	A. Yes (T1, T2) B. No (#T1, #T2) C. Not applicable	AUISM Security Control: 1436, revision 1 NZISM 10.8 NZISM 22.2 NIST 800-171 3.1.3

1.2.3 Security | Technical (continued...)

#	Question	Tier	Response Options	Standard
S5	Are all of the service's web servers secured with digital certificates signed by a reputable trusted authority?	1 & 2	A. Yes (please specify CA) (T1, T2) B. No (#T1, #T2)	NZISM 17.1 NZISM 17.2 NIST 800-171 3.13.15
S6	Does your organisation have a documented and implemented key management process which describes at a minimum: • Key generation; • Key registration; • Key storage; • Key distribution and installation; • Key use; • Key rotation; • Key backup; • Key recovery; • Key revocation; • Key suspension; and • Key destruction?	1	A. No - none of the above B. Yes - some of the above C. Yes - all of the above (T1)	NZISM 17.9 NIST 800-171 3.13.10
S7	Are production servers (e.g., authentication servers, Domain Name System (DNS), web servers, file servers and email servers), containers, serverless services and all end points protected by HIPS (Host-based Intrusion Prevention System), software-based application fire-walls, anti-virus and anti-malware all of which are kept up to date with definitions and maintained?	1 & 2	A. No - none of the above B. Yes - some of the above C. Yes – all of the above except HIPS (T2) D. Yes - all of the above (T1)	AUISM Security Controls: 1341, 1034, 1416, 1417 NZISM 14.1 NZISM 18.4 NIST 800-171 3.4.6 CIS 10.1

1.2.3 Security | Technical (continued...)

#	Question	Tier	Response Options	Standard
S8	Does your organisation enforce the following controls on database management system (DBMS) software: • Follow vendor guidance for securing the database; • DBMS software features and stored procedures, accounts and databases that are not required are disabled or removed; • Least privileges; • File-based access controls; • Disable anonymous and default database administrator account; • Unique username and password for each database administrator account; • Use database administrator accounts for administrative tasks only; and • Segregate test and production environment?	1 & 2	A. No - none of the above (#T1, #T2) B. Yes - some of the above C. Yes - all of the above (T1, T2)	AUISM Security Controls: 1246, 1247, 1249, 1250, 1260, 1262, 1263, 1273 NZISM 20.4 NZISM 14.1 NZISM 10.8
S9a	Are internet facing components (e.g., web servers) separated from other online components (e.g. databases) using the following controls: • Secure communication between network segments (e.g., using firewalls), including filtering between network segments • DMZ for internet-facing components and separate trusted zones for other components • Virtual (e.g., VLAN) or physical network segregation	1 & 2	A. No – none of the above (#T1) B. Partial – secure communication or DMZ C. Partial – virtual or physical network segregation (T2) D. Yes – all of the above (T1, T2)	AUISM Security controls: 1181, 1577, 1532, 0529, 1364, 0535, 0530, 0520, 1182, 0385, 1479, 1006, 1437, 1436, 0628 NZISM 10.8 NZISM 14.1.11 NZISM 19.1 NZISM 22.2 NIST 800-171 3.1.3

1.2.3 Security | Technical (continued...)

#	Question	Tier	Response Options	Standard
S9b	Within the organisation, for internal systems and components (e.g. databases, internal user networks) that routinely deal with sensitive data or are widely accessed, is there a separation between internet facing components and other online components?		A. Yes (T1, T2) B. No	NIST 800-171 3.13.1 NIST 800-171 3.13.5
S9c	For the service, is a separate, sand-boxed execution domain maintained for each executing system process?		A. Yes (T1, T2) B. No	NIST 800-53 SC-39
S9d	For the service, is system memory protected from unauthorized code execution (e.g. data execution prevention, address space layout randomization)?		A. Yes (T1, T2) B. No	NIST 800-53 SI-16 (DESIRABLE)
S10	Does your organisation have a documented and implemented system hardening process which: • Includes in scope operating systems, virtualization platforms, storage, network, software, applications, workstations and other end-user devices (including portable, mobile and IoT devices); • Includes the management of default user accounts and access levels and the uninstallation or disablement of the unnecessary services; • Ensures only required ports, protocols, services and authorizations are enabled, whether for internal or external connections; • Is reviewed annually and when significant changes occur, including when system components are installed or upgraded; • Results in security configurations being established and enforced for organisation systems; and • Ensures only required and authorized software is installed and used.	1 & 2	A. No – none of the above (#T1, #T2) B. Yes – some of the above C. Yes – all of the above except annual review (T2) D. Yes – all of the above (T1)	AUISM Security Control: 1406 Revision: 2; Security Control: 1585 Revision: 0; Security Control: 1605 Revision: 0; Security Control: 1588 Revision: 0. NZISM 14.1 NZISM 22.2 NIST 800-171 3.4.2 NIST 800-171 3.4.6 NIST 800-171 3.4.7 NIST 800-171 3.4.8 NIST 800-171 3.4.9 NIST 800-53 CM-2(1) NIST 800-53 CM-2(7) (DESIRABLE) NIST 800-171 3.7.3 NIST 800-53 CA-9 NIST 800-171 3.13.6 NIST 800-171 3.14.7 CIS 2.3, 4.1, 4.2

1.2.3 Security | Technical (continued...)

#	Question	Tier	Response Options	Standard
S10A	Does your organisation enforce enhanced security configurations for organisation systems and components moving: • Physically to high-risk areas; and • Off-site for maintenance.		A. No - none of the above B. Yes - some of the above C. Yes - all of the above (T1, T2)	NIST 800-53 CM-2(7), NIST 800-171 3.7.3
S11	Has your organisation implemented the following perimeter controls: • External firewall; • Host based firewalls or port filtering on end-user devices with default-deny rules; • IDS/IPS (Intrusion Detection System/ Intrusion Prevention System); • DMZ (Demilitarized Zone) for hosting external sites; • Content filtering (including blocking of unnecessary file types); • DoS/DDoS (Denial of Service / Distributed Denial of Service) defense; • Web Application Firewall (WAF); • Filtering and monitoring of outgoing traffic (spikes, unusual activity, malicious content); • Packet inspection; • Network segmentation; • VPN required for remote access; • Detection and monitoring of unauthorized devices on the network through both passive and active device discovery, resulting in updates to asset inventory on a regular basis; • DNS filtering and network URL based filters; and • Organisation assets are configured to use trusted DNS servers? • explicit restrictions on information transfer to external systems based on data structures and content, as well as authorization (for example, enforcing read-only access, filtering, message security tagging and reclassification of message security) • Authorization and encryption on the organization's wireless network?	1 & 2	A. No - none of the above (#T1, #T2) B. Yes - some of the above C. Yes - all of the above except for Web Application Firewall (WAF) (T2) D. Yes - all of the above (T1)	AUISM Security Control: 1528 Revision: 1; Security Control: 1435; Revision: 1. NZISM 10.8 NZISM 18.4 NZISM 19.1 NZISM 19.3 NIST 800-171 3.1.3 NIST 800-171 3.1.13 (DESIRABLE) NIST 800-171 3.1.14 (DESIRABLE) NIST 800-171 3.1.16 (DESIRABLE) NIST 800-171 3.1.17 (DESIRABLE) NIST 800-171 3.1.21 (OPTIONAL) NIST 800-171 3.13.7 NIST 800-171 3.13.9 NIST 800-53 SC-7(3) NIST 800-53 SC-7(4) NIST 800-53 SC-20 NIST 800-53 SC-21 NIST 800-53 SC-22 NIST 800-171 3.14.6 NIST 800-171 3.14.7 CIS 4.4, 4.5, 9.2 UKCE A2.8 UKCE A4.1 - 4.5 UKCE A4.6 - 4.12

1.2.3 Security | Technical (continued...)

#	Question	Tier	Response Options	Standard
S11	• Restrictions on the use of portable storage devices to transfer information from organisation systems to external systems • Blocking of split tunnelling • Automatic termination of inactive network connections at the end of a session or after a defined period of inactivity • Implemented traffic flow policy on each external telecommunications service used; • Prevent unauthorized use of control plane traffic (e..g Border Gateway Protocol routing, Domain Name System) • Data origin authentication and Integrity verification on name/address resolution services such as DNS, including child zone • Fault tolerance on name/address resolution services such as DNS, including secondary server and internal/external server separation • Periodic scan of organisational file storage and real-time scans of files from external sources	1 & 2	A. No - none of the above (#T1, #T2) B. Yes - some of the above C. Yes - all of the above except for Web Application Firewall (WAF) (T2) D. Yes - all of the above (T1)	AUISM Security Control: 1528 Revision: 1; Security Control: 1435; Revision: 1. NZISM 10.8 NZISM 18.4 NZISM 19.1 NZISM 19.3 NIST 800-171 3.1.3 NIST 800-171 3.1.13 (DESIRABLE) NIST 800-171 3.1.14 (DESIRABLE) NIST 800-171 3.1.16 (DESIRABLE) NIST 800-171 3.1.17 (DESIRABLE) NIST 800-171 3.1.21 (OPTIONAL) NIST 800-171 3.13.7 NIST 800-171 3.13.9 NIST 800-53 SC-7(3) NIST 800-53 SC-7(4) NIST 800-53 SC-20 NIST 800-53 SC-21 NIST 800-53 SC-22 NIST 800-171 3.14.6 NIST 800-171 3.14.7 CIS 4.4, 4.5, 9.2 UKCE A2.8 UKCE A4.1 - 4.5 UKCE A4.6 - 4.12
S12	Has your organisation documented and implemented a security policy governing the management and connectivity of mobile devices, including • use of a Mobile Device Management solution applied to all mobile devices and • encryption of any sensitive information transferred to mobile devices?	1 & 2	A. No - none of the above B. Policy documented and implemented, but MDM not applied to all devices C. Yes - all of the above (T1)	NZISM 21.1 NZISM 21.4 NIST 800-171 3.1.18 (OPTIONAL) NIST 800-171 3.1.19 (OPTIONAL) CIS 3.6

1.2.3 Security | Technical (continued...)

#	Question	Tier	Response Options	Standard
S12a	Has your organisation documented and implemented a security policy governing the management and use of externally owned systems and devices, such as personally owned computers, portable storage devices and removable media (including media used for system maintenance) and does this policy include: • physically controlling and securely storing all media (paper and digital) containing sensitive data; • restricting access to media containing sensitive data to authorized staff; • encrypting any sensitive data on media that is moved outside secure areas (including external work sites and work from home); • logging any transport of media outside secure areas; • marking media containing sensitive data with applicable distribution limitations; • requiring all removable portable storage devices to have an identifiable owner; • disabling all autorun and auto-play functionality on removable media?	1 & 2	A. No - none of the above B. Yes - some of the above (T2) C. Yes - all of the above (T1)	NIST 800-171 3.1.20 (OPTIONAL) NIST 800-171 3.7.4 NIST 800-171 3.8.1 NIST 800-171 3.8.2 NIST 800-171 3.8.4 (DESIRABLE) NIST 800-171 3.8.5 (DESIRABLE) NIST 800-171 3.8.6 (DESIRABLE) NIST 800-171 3.8.7 NIST 800-171 3.8.8 NIST 800-53 MP-1 NIST 800-171 3.10.6 CIS 10.3 UKCE A5.1 - 5.3 UKCE A8.1 - 8.5
S13	Is production data used in non-production (e.g., test and development) environments?	1 & 2	A. Yes – without identical security controls applied and de-identification of production data. (#T1, #T2) B. Yes - with identical security controls applied and/or with production data de-identified C. No (T1, T2), production data (even if de-identified) is not used in testing or development at all	AUISM Security Control: 1420 Revision: 2. NZISM 14.4 NZISM 20.1 UKCE A2.7

1.2.3 Security | Technical (continued...)

#	Question	Tier	Response Options	Standard
S13	Is production data used in non-production (e.g., test and development) environments?	1 & 2	A. Yes – without identical security controls applied and de-identification of production data. (#T1, #T2) B. Yes - with identical security controls applied and/or with production data de-identified C. No (T1, T2), production data (even if de-identified) is not used in testing or development at all	AUISM Security Control: 1420 Revision: 2. NZISM 14.4 NZISM 20.1 UKCE A2.7
S14	Does your organisation: • disable the internal use of business productivity tool macros (e.g., Microsoft Office macros) and scripts (VB, java, PowerShell) for users that don't have a demonstrated business requirement; • block macros in files originating from the internet; • enable macro antivirus scanning; and • ensure macro security settings can't be changed by users?	1 & 2	A. No B. Yes – some of the above C. Yes – all of the above (T1, T2) D. N/A (T1, T2)	AUISM Security Controls: 1487, 1488, 1489 NZISM 20.3
S15	Are all of the organisation's desktop computers, laptops, tablets, mobile phones and other devices protected from viruses and malware by: • Having anti-virus and anti-malware installed; • Limiting the applications and services which can be installed to a documented approved set; • Anti-virus and anti-malware signatures are updated at least daily; • Anti-virus and anti-malware scan files automatically before access; and • Anti-virus and anti-malware scan web pages and provide warnings to users when malicious sites are accessed?	1 & 2	A. No B. Yes – some of the above C. Yes – all of the above (T1, T2) D. N/A (T1, T2)	NZISM 14.1, CIS 10.1 to 10.7

1.2.4 Security | Logging

Criteria around how and how much the product logs events relevant to security.

#	Question	Tier	Response Options	Standard
L1	Does your organisation have a documented and implemented logging procedure, covering collection, review and retention, which is reviewed annually and which requires all systems both in your organisation (e.g., servers, storage, network, applications, etc.), and specifically in your product, to log the following and synchronize logs to a consistent time source: • Authentication logs (e.g., successful login, unsuccessful login, logoff) • Privileged operations logs (e.g., access to logs, changes to configurations or policy, failed attempts to access data and resources) • User administration logs (e.g., addition/ removal of users, changes to accounts, password changes) • System logs (e.g., system shutdown/ restarts, application crashes and error messages) • Used or ascribed a unique identifier of the user who has performed the activity being logged	1 & 2	A. No - none of the above B. Yes - some of the above (T2) C. Yes - all of the above (T1)	AUISM Security Controls: 0584, 0585, 0582, 1536, 1537 NZISM 16.6 NIST 800-171 3.1.7 NIST 800-171 3.3.1 NIST 800-171 3.3.2 NIST 800-171 3.3.7 NIST 800-53 MA-4(2) NIST 800-53 AU-2 CIS 8.1
L2	Does your organisation have a documented and implemented event log auditing procedure which outlines, at a minimum: • Schedule of audits (annual or real-time for sensitive data); • Definitions of security violations; • Actions to be taken when violations are detected; and • Reporting requirements?	1 & 2	A. No B. Yes - all of the above without real-time monitoring (T2) C. Yes - all of the above with real-time monitoring (T1)	AUISM Security Control: 0109 NZISM 7.1.7 NZISM 16.6 NIST 800-171 3.3.5 (DESIRABLE) NIST 800-171 3.3.6 (DESIRABLE) NIST 800-53 AU-6 NIST 800-53 CA-7
L3	Will you supply all relevant audit and logging data in response to customer requests?	1 & 2	A. No B. Yes (T1, T2)	
L4	Has your organisation implemented a centralized logging facility to store logs which: • Ensure logs cannot be tampered with; • Triggers an alert in case a logging transaction fails; • Supports audit reduction and report generation for analysis; and • Ensures adequate storage to comply with specified retention times?	1	A. No B. Yes (T1)	AUISM Security Control: 1405 NZISM 16.6} NZISM 18.4.12 NIST 800-171 3.3.1 NIST 800-171 3.3.4 NIST 800-171 3.3.6 (DESIRABLE) NIST 800-171 3.3.8 CIS 8.3

1.2.5 Security | Access

Criteria around the constraints and controls realized for who gains access to the product and its data.

#	Question	Tier	Response Options	Standard
A1	Are all users (including administrators, system accounts, and devices), uniquely identifiable within the service (i.e., via unique usernames and appropriately robust passwords)?	1 & 2	A. No (#T1, #T2) B. Yes (T1, T2)	AUISM Security Control: 0414 NZISM 16.1 NIST 800-171 3.5.1 UKCE A4.2 UKCE A4.4 UKCE A4.5 UKCE A4.8 - 4.10 UKCE A5.9 UKCE A5.10 UKCE A7.1 - 7.5 UKCE A7.7 UKCE A7.10 UKCE A7.12 UKCE A7.14
A1a	Does all access to the service require authentication and authorization, including both human access, and access by process or devices?	1 & 2	A. No (#T1, #T2) B. Yes (T1, T2)	NIST 800-171 3.1.1 NIST 800-171 3.5.2
A1b	Within the organisation, are all accounts disabled after 45 days of inactivity and are user identifiers blocked from reassignment to new users for a defined period of time?	1 & 2	A. No B. Yes (T1, T2)	NIST 800-171 3.5.5 NIST 800-171 3.5.6 (DESIRABLE) CIS 5.3 UKCE A4.6 UKCE A7.3
A1c	Across the organisation is there an inventory of all user, administrator and service accounts, which includes details of the person's name (if applicable), username/identifier, start/stop dates, and department (if an employee), and is this inventory of accounts validated at least every 3 months?	1 & 2	A. No B. Yes (T1, T2)	CIS 5.1 UKCE A7.1 UKCE A7.4 - 7.9
A2	Are all passwords used to access the service (i.e. user, system, and privileged account passwords) protected in line with the recommendations of at least one of: the Australia Cyber Security Centre Information Security Manual; New Zealand Information Security Manual, UK NCSC Cybersecurity Body of Knowledge (CyBoK) and/or Open Web Application Security Program's Application Security Verification Standard V2.4 Credential Storage Requirements, including the recommendation for ensuring passwords are hashed, salted and stretched?	1 & 2	A. No (#T1, #T2) B. Yes for all users – excluding students (T1, T2). Please detail why this exception is required and specify any controls in place for student accounts. C. Yes for all users (T1, T2)	AUISM Security Control: 1252 NZISM 16.1 NZISM 16.1.41 NIST 800-171 3.5.10 (DESIRABLE)

1.2.5 Security | Access (continued...)

#	Question	Tier	Response Options	Standard
A2a	Are passwords obscured or masked as users enter them in order to access the service?	1 & 2	A. No B. Yes (T1, T2)	NIST 800-171 3.5.11
A3	At a minimum, are the following password requirements enforced for vendor staff, external contractors or associates with access to the organisation's systems and the service: • if using single factor authentication, passwords are a minimum of 14 characters with controls that limit predictability (inc. complexity) • if using multi-factor authentication, passwords are a minimum of eight characters	1 & 2	A. No B. Yes (T1, T2)	AUISM Security Control: 0421, 1559 NZISM 16.1 NIST 800-171 3.5.7 CIS 5.2 UKCE A7.10 - 7.17
A3a	Does the service limit unsuccessful logon attempts, e.g. by resetting the user password after several such attempts?	1 & 2	A. No B. Yes (T1, T2)	NIST 800-171 3.1.8 UKCE A7.10 - 7.13
A4	Within the service, do you offer multi-factor authentication for end-users?	1 & 2	A. No B. Yes, offered as an option (T1) C. Yes, mandated for end users (T1)	AUISM Security Control: 0974 NZISM 16.1 NZISM 21.4.11 NIST 800-171 3.5.3 UKCE A7.14 - 7.17
A4a	Within the service, is the multi-factor authentication used relay-resistant (e.g. nonces, one-time authentication tokens)?	1 & 2	A. No B. Yes (T1, T2) C. N/A Multifactor not supported	[NIST 800-171 3.5,4] (Required in Australian and Open Web but not New Zealand controls)
A5	Does your organisation mandate multi-factor authentication for: • Vendor staff, external contractors or associates accessing systems remotely (including access to cloud systems); • System administrators; • Support staff; • Staff with privileged accounts?	1 & 2	A. No – none of the above (#T1) B. Yes – some of the above (#T1) C. Yes – all of the above (T1, T2)	AUISM Security Control: 1173 Revision 3 NZISM 16.4 NZISM 16.7 NZISM 19.1.20 NZISM 21.4.11 NIST 800-171 3.1.15 (DESIRABLE) NIST 800-171 3.5.3 CIS 6.4, 6.5 UKCE A7.16

1.2.5 Security | Access (continued...)

#	Question	Tier	Response Options	Standard
A5a	Within your organisation, are additional authorization protocols required to execute privileged commands remotely, compared to on-site?	1 & 2	A. No B. Yes (T1, T2)	NIST 800-171 3.1.15 (DESIRABLE) NIST 800-171 3.7.5 (DESIRABLE)
A5b	Within your organisation, does the secure management of enterprise assets and software occur via one or more of the following: • Version controlled infrastructure as code; or • Accessing administrative interfaces securely via SSH or HTTPS?	1 & 2	A. No B. Yes (T1, T2)	CIS 4.6
A5c	Across your organisation, are all externally exposed enterprise or third-party applications required to enforce multi-factor authentication?	1 & 2	A. No B. Yes (T1, T2)	CIS 6.3 UKCE A7.16
A6	Does your organisation provide access to systems based on roles (e.g., role-based access control (RBAC)), and is this process documented for all systems including the service?	1 & 2	A. No (#T1) B. Yes, for some systems C. Yes, for all systems (T1, T2)	NZISM 16.2 NZISM 16.4 NIST 800-171 3.1.1 NIST 800-171 3.1.2 UKCE A7.1 UKCE A7.4
A6a	With regards to the development of the service, are different mission, testing, auditing, and system support roles allocated to different individuals (organisation staff, vendor staff, external contractors, associates) as a matter of policy	1 & 2	A. No B. Yes (T1, T2)	NIST 800-171 3.1.4 NIST 800-171 3.1.9 UKCE A7.4
A7	At a minimum, are vendor staff, external contractors or associates with access to systems, applications and information (including audit logs): • Validated and approved by appropriate personnel; • Periodically reviewed (at least annually) and revalidated or revoked; and • Reviewed and revalidated or revoked following changes to role, employment and/or inactivity? • Provided appropriate security notices when they access the system	1 & 2	A. No (#T1) B. Yes (T1, T2)	AUISM Security Controls: 0405, 0430, 1404 NZISM 16.3 NZISM 16.5 NIST 800-171 3.1.9 (DESIRABLE) NIST 800-171 3.9.2UKCE A7.3

1.2.5 Security | Access (continued...)

#	Question	Tier	Response Options	Standard
A8	Do your support staff require remote access to end user devices?	1 & 2	A. Yes (please specify) B. No (T1, T2)	
A8a	Is privileged system management segregated from user functionality? (e.g. through different computers, different operating systems, use of VPNs)	1 & 2	A. No B. Yes (T1, T2)	NIST 800-171 3.13.3
A9	Are vendor staff, external contractors or associates with non-privileged accounts restricted from installing, uninstalling, disabling or making any changes to software and system configuration on servers and endpoints?	1 & 2	A. No B. Yes (T1, T2)	AUISM Security Control: 1584, 1491 NZISM 14.1 NIST 800-171 3.4.2 NIST 800-171 3.4.5 NIST 800-171 3.7.2 NIST 800-171 3.7.6
A10	Are all internal organisation systems (including operating systems) configured with a session or screen lock that: • activates after a maximum of 15 minutes of user inactivity or if manually activated by the user; • activates after a maximum of 2 minutes of user inactivity or if manually activated by the user for mobile end-user devices; • completely conceals all information on the screen; • ensures that the screen does not enter a power saving state before the screen or session lock is activated; • requires the user to reauthenticate to unlock the system; and • denies users the ability to disable the session or screen locking mechanism? • does not display any secure information of its own	1 & 2	A. No (#T1) B. Yes, some of the above C. Yes, all of the above (T1, T2)	AUISM Security Control: 0428 NZISM 16.1.45 NIST 800-171 3.1.10 CIS 4.3 UKCE A5.10
A10a	For the service, are user log-in sessions automatically terminated after a period of inactivity, or in response to a security incident?	1 & 2	A. No B. Yes (T1, T2)	NIST 800-171 3.1.11 (DESIRABLE) UKCE A5.9

1.2.5 Security | Access (continued...)

#	Question	Tier	Response Options	Standard
A11	When a password reset is requested by the user or enforced by the service, are: • the newly assigned passwords (e.g., temporary initial passwords) randomly generated; • users required to provide verification of their identity (e.g., answering a set of challenge-response questions); • new passwords provided via a secure communication channel or split into parts; and • users required to change their assigned temporary password on first use?	1 & 2	A. No (#T1) B. Yes, some of the above C. Yes, all of the above (T1, T2) D. N/A - Password resets do not occur	AUISM Security Controls: 1227, 1593, 1594, 1595 NZISM 16.1.41 NZISM 16.1.42 NIST 800-171 3.5.9 (DESIRABLE) UKCE A5.3 UKCE A5.6
A11a	For the service, when a new password is selected by a user, is there a restriction on: • How similar the new password is to the previous password; • The time duration or number of password changes before a previous password can be reused by a user?	1 & 2	A. No B. Yes (T1, T2)	NIST 800-171 3.5.7 NIST 800-171 3.5.8 (DESIRABLE) UKCE A7.10 - 7.12
A12	Does the service allow user registration or logon/authentication or Single Sign-on (SSO) via credentials provided by another Identity Provider (IDP) such as RealMe, Facebook, Google, Microsoft etc.	1 & 2	A. Yes (please specify). B. No (T1, T2)	
A13	What is the service's approach to default user access permissions (e.g., all access is denied unless specifically allowed based on a need to know, all access is allowed unless specifically denied)?	1 & 2	A. Protection by exception (Allow access unless specifically denied) (#T1) B. Protection by default (Deny unless approved) (T1, T2)	UKCE A7.4
A13a	In your organisation, are privileged accounts ("super-users") managed by a documented and implemented process and are non-privileged users prevented from executing privileged functions?	1 & 2	A. No B. Yes (T1, T2)	NIST 800-171 3.1.5 NIST 800-171 3.1.7 UKCE A7.5 - 7.9
A13b	In your organisation, is the use of privileged accounts (administrators/super-users) restricted by policy to only those functions that require privileged access, and for the duration of those functions? (This includes external maintenance operations.	1 & 2	A. No B. Yes (T1, T2)	NIST 800-171 3.1.6 (OPTIONAL) NIST 800-171 3.7.5 (DESIRABLE) CIS 5.4 UKCE A7.4 - 7.9

1.2.5 Security | Access (continued...)

#	Question	Tier	Response Options	Standard
A13c	In your organisation, are data access control lists: • Implemented; • configured based on a user's need to know; and • are these controls applied to local and remote file systems, databases and applications?	1 & 2	A. No B. Yes (T1, T2)	CIS 3.3
A14	Does the service support Single Sign-On (SSO)?	1 & 2	A. No B. Yes – Optional. Please specify SSO supported. C. Yes – Mandatory. Please specify SSO supported.	
A16A	Does the service require, suggest or imply that accounts be created in any third-party services (whether subcontractors or independent third parties) for any purpose whatsoever (data collection, data exchange, other)?	1 & 2	A. No B. Yes	
A16B	In relation to the creation of accounts in third party services, are enforceable written agreements in place with all of these third-party services covering this arrangement?	1 & 2 Conditional (A15 – yes)	A. No (#T1, #T2) B. Yes (T1, T2)	
A16C	Who creates the account/s in the third-party service?	1 & 2 Conditional (A15 – yes)	A. The school, school system, or jurisdiction B. The third-party service C. The service (responding to this assessment)	

1.2.5 Security | Access (continued...)

#	Question	Tier	Response Options	Standard
A17	Within the vendor organisation, is application control: • Implemented on all workstations; • Implemented on internet-facing and non-internet facing servers; • Enabled to restrict the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set; • Enabled to restrict the execution of drivers to an organisation-approved set; • Implemented using cryptographic hash rules, publisher certificate rules or path rules; • Rule sets are validated on an annual or more frequent basis; • When implementing application control using publisher certificate rules, both publisher names and product names are used; and • Extended to tools and applications used in system and software maintenance;	1 & 2	A. No, none of the above B. Yes, some of the above C. Yes, all of the above (T1, T2)	AUISM Security Controls: 0843, 1490, 1656, 1657, 1658, 0955, 1582, 1471 NZISM 14.2 NIST 800-171 3.7.2 NIST 800-171 3.13.13

1.2.6 Security | HR

Criteria around the steps taken by the organisation to ensure security-compliant behavior by its staff.

#	Question	Tier	Response Options	Standard
HR1	Do all vendor staff, external contractors and associates who have access to user data or user content undergo employment screening (e.g., criminal history checks, working with children checks) as per applicable regulatory requirements?	1 & 2	A. No (#T1) B. Yes (T1, T2)	AUISM Security Control: 0434 NZ PSR PERSEC1 NIST 800-171 3.9.1
HR1b	Within your organisation, where agreements are required to be signed by vendor staff, external contractors and associates who have access to user data or user content are: • the individuals required to re-sign those agreements when they are updated; and • do those agreements provide for sanctions for failure to comply; and • is there formal notification given when a sanctions process is initiated?		A. Not applicable – agreements are not required to be signed B. No, none of the above C. Yes, some of the above D. Yes, all of the above (T1, T2)	NIST 800-53 PS-8

1.2.6 Security | HR (continued...)

#	Question	Tier	Response Options	Standard

HR2	Does your organisation run, based on the staff member's role, a customized security, privacy and online safety awareness / education program which addresses the following at a minimum:
	• Identification of who the awareness training needs to be delivered to, with records kept of training for each individual;
	• Identification, documentation and monitoring of when awareness training needs to be delivered (e.g., during induction, annually, etc.);
	• Identification of how the awareness training is to be delivered (e.g., classroom training, online course, security awareness posters, emails, etc.);
	• The content to be delivered for each awareness session such as:
	  • Basic understanding of the need for information security, privacy and online safety, including causes of unintentional data exposure;
	  • Actions to maintain security, privacy and online safety, including practical office/desktop practices;
	  • Actions to respond to suspected security, privacy and online safety incidents;
	  • Applicable policies and laws;
	  • Practical security, privacy and online safety awareness exercises;
	  • Data identification and storage, including the safe transfer of data, archival and destruction;
	  • Disciplinary actions for significant security and privacy breaches by staff;
	  How to recognize and report indicators of potential insider threats to security by staff.;
	  Covers recognizing social engineering attacks such as phishing, pre-texting and tailgating; and
	  • Covers authentication best practices including MFA, password composition and managing credentials;
	  • Covers verifications and reporting of out-of-date software patches and any failure in automated processes and tools; and
	  • Covers the dangers of connecting to, and transmitting data over insecure networks for business activities, with specific training for remote workers regarding safe configuration of home networks.
		1 & 2	A. No - none of the above (#T1)
			B. Yes - some of the above
			C. Yes - all of the above (T1, T2)
				AUISM Security Control: 0252
				NZISM 9.1
				NZISM 3.2.18
				NZISM 3.3.13
				NZISM 7.1.7
				NIST 800-171 3.2.1
				NIST 800-171 3.2.2
				NIST 800-171 3.2.3
				NIST 800-53 AT-4
				[OPTIONAL]
				CIS 14.1, 14.2, 14.3, 14.4, 14.5, 14.6, 14.7, 14.8

1.2.6 Security | HR (continued...)

#	Question	Tier	Response Options	Standard
HR3	Is there a documented and implemented process to remove access to systems, applications and data repositories for personnel (vendor staff, external contractors and associates) that: • no longer have a legitimate requirement for access (implemented on the same day); and • are detected undertaking malicious activities (implemented immediately)?	1 & 2	A. No (#T1) B. Yes – but not implemented within required timeframes C. Yes – (T1, T2)	AUISM Security Control: 0430, 1591 NZISM 16.1.46 NZISM 16.4.33
HR4	Is there a documented and implemented process to grant access to systems, applications and data repositories for new personnel (vendor staff, external contractors and associates) or when a user changes roles?		A. No B. Yes – (T1, T2)	CIS 6.1

1.2.7 Security | Processes and Testing

Criteria to ensure that the organisation has ongoing processes to ensure security on its systems.

#	Question	Tier	Response Options	Standard
T1	Does your organisation have an implemented continuous monitoring plan for all organisational systems and infrastructure that includes: • conducting vulnerability scans for systems at least monthly • conducting penetration tests for systems after a major change or at least annually • analyzing identified security vulnerabilities to determine their potential impact and appropriate mitigations based on effectiveness, cost and existing security controls • using a risk-based approach to prioritize the implementation of identified mitigations with at least monthly review • conducting vulnerability scans for systems when significant new vulnerabilities affecting those systems are identified; conducting vulnerability scans using tools that can be and are readily updated for new vulnerabilities to be scanned • update vulnerability scans in response to security alerts as they are published, including updated anti-virus and anti-malware signatures • Reviewing and updating the plan annually or when significant changes occur	1 & 2	A. No (#T1, #T2) B. Yes - meets all of the requirements above but conducted less frequently C. Yes - meets all requirements above (T1, T2) D. Yes – meets all requirements above including the use of external independent resources to conduct penetration testing (T1, T2)	AUISM Security Control: 1163 NZISM 4.1.26-29 NZISM 4.3 NZISM 6.1-6.2 NZISM 14.4-14.5 NIST 800-171 3.11.2 NIST 800-171 3.11.3 NIST 800-53 RA-5(1) NIST 800-53 RA-5(2) NIST 800-171 3.12.2 NIST 800-171 3.12.3 NIST 800-53 CA-7 NIST 800-171 3.14.1 NIST 800-171 3.14.3 NIST 800-171 3.14.4 NIST 800-53 SI-4(5) CIS 7.1, 7.2, 10.2, 18.1 UKCE A6.4 UKCE A6.5 UKCE A8.1 to 8.5
T1b	Does your organisation monitor compliance of third party providers which make up your solution for compliance with your organisation's security and privacy requirements?		A. No B. Yes (#T1, #T2)	NIST 800-SA9
T1c	Does your organization have a vulnerability disclosure program providing authorization for security researchers to test for and report vulnerabilities?		A. No	NIST 800-53 RA-5(11) AUISM 1616/1755/1756 NZISM 5.9

1.2.7 Security | Processes and Testing (continued...)

#	Question	Tier	Response Options	Standard
T2	Does your organisation use a centrally managed approach to patch, update or otherwise maintain applications, drivers, operating systems, and firmware and hardware which includes ensuring: • the integrity and authenticity of patches; • successful application of patches; • that patches remain in place; and • that the list of supported software for updates is reviewed regularly; and - that by default, patches to the product are applied automatically i.e. without the need for customer action		A. No – none of the above (#T1) B. Yes – some of the above C. Yes – all of the above (T1, T2)	AUISM Security Controls: 0298 revision 7, 0303, 1499, 1497, 1500. NZISM 12.4 NZISM 14.5.8 NIST 800-171 3.7.1 CIS 2.2, 7.3, 7.4 UKCE A6.4 UKCE A6.5
T3	Are patches, updates or vendor mitigations for security vulnerabilities in: • internet facing services (including operating systems of internet-facing services); • workstation, server and network device operating systems; • operating systems of other ICT equipment; and • drivers and firmware; • applied within two weeks of release, or within 48 hours if an exploit exists?	1	A. No (#T1) B. Yes (T1, T2)	AUISM Security Controls: 1690, 1694, 1695, 1696, 1751, 1697 NZISM 12.4 NIST 800-3.14.1 CIS 7.3, 12.1 UKCE A6.4 UKCE A6.5
T4	Are patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software and security products applied within two weeks of release, or within 48 hours if an exploit exists?	1 & 2	A. No B. Yes (T1, T2)	AUISM Security Control: 1691, 1692 NZISM 12.4 NIST 800-3.14.1 CIS 7.4 UKCE A6.4 UKCE A6.5
T5	Are patches, updates or vendor mitigations for security vulnerabilities in other applications applied within one month of release?	1 & 2	A. No B. Yes (T1, T2)	AUISM Security Controls: 1693 NZISM 12.4 NIST 800-3.14.1 CIS 7.4

1.2.7 Security | Processes and Testing (continued...)

#	Question	Tier	Response Options	Standard

T6	Does your organisation have a formal, documented and implemented incident response plan which requires security, privacy and online safety incidents to be:
	• Identified, following a clear definition;
	• Reported by staff (if internal);
	• Proactively monitored;
	• Contained;
	• Investigated;
	• Remediated;
	• Tracked with metrics, to measure response effectiveness; and
	• Recorded in a register with the following information at a minimum:
	  • Date incident occurred;
	  • Date incident discovered;
	  • Description of the incident;
	  • Actions taken in response to the incident; and
	  • Name of person to whom the incident was reported?
		1 & 2	A. No - none of the above (#T1, #T2)
			B. Yes - some of the above (T2)
			C. Yes - all of the above (T1)
				AUISM Security Control: 0125
				NZISM 7.1-7.3
				NZISM 5.6
				NZISM 22.1.25
				NIST 800-171 3.6.1
				NIST 800-53 IR-8
				CIS 17.2, 17.3

T6a	Is the incident response capability of the organisation regularly tested and reviewed?	1 & 2	A. No B. Yes (T1, T2)	NIST 800-171 3.6.3 (DESIRABLE)
T6b	As part of your organisation's incident handling process does your organisation: • have one key person and at least one backup tasked with managing the organisation's incident handling process; and • have contact information for all parties that need to be informed of security incidents (e.g. staff, third party vendors, law enforcement, insurance providers, government agencies etc); and • contacts are updated annually?	1 & 2	A. No B. Yes (T1, T2)	CIS 17.1
T7	When a data breach occurs, are affected customers and organisations, and the relevant authorities, notified as soon as possible after a data breach is discovered and given all relevant details (including affected individuals and what information was disclosed)?	1 & 2	A. No B. Yes (T1, T2)	AUISM Security Controls: 0123, 0141, 0140 NZISM 7.2 NZPP-5 NZISM 7.2.22 NZPP NIST 800-171 3.6.2
T8	When a data loss/corruption event occurs, are affected customers and/or organisations notified as soon as possible after this is discovered and given all relevant details?	1 & 2	A. No – none of the above B. Yes – some of the above (T2) C. Yes – all of the above (T1, T2)	AUISM Security Controls: 0123, 0141, 0140 NZISM 7.2 NZPP-5 NIST 800-171 3.6.2

1.2.8 Security | Plans and Quality

Criteria around the adoption by the organisation of explicit plans and policies to ensure ongoing security compliance and software quality.

#	Question	Tier	Response Options	Standard
Q1	(Question removed from 2021.1)			
Q2	Does your organisation have a documented and implemented Business Continuity Plan for the service, which is updated annually or when significant changes occur, covering: • Backup strategies (including automated backups at least weekly or more frequently as required and back-ups that are stored disconnected); • Restoration strategies (e.g., disaster recovery), including prioritization; • Preservation strategies; • And considers the security of backed up data?	1	A. No B. Yes - meets some requirements C. Yes - meets all requirements (T1)	AUISM Security Controls: 1547, 1548, 1510 NZISM 6.4 CIS 11.1, 11.2
Q3	Does your organisation have a documented and implemented IT Change management process and supporting procedures which includes the following at a minimum: • Applicable criteria for entry to and exit from the change management process • Categorization of IT change (e.g., Standard, Pre-Approved, Emergency, etc.); • Approval requirements for each category of IT change; • Assessment of potential security impacts; • Prerequisites for the IT change (e.g., the IT change has been tested in a non-production environment); • Documentation requirements in regard to the change (e.g., completion of a template in an IT change management tool, completion of a rollback plan, etc.); • Documentation that needs to be updated as a result of the change (e.g., as-built documentation, IT Disaster Recovery Plans, etc.); • IT change communication processes (e.g., notifications to users); and • Validations are required for all changes to systems before they are finalized	1 & 2	A. No change management process B. Yes, change management process meets some requirements C. Yes, change management process meets all requirements (T1, T2)	AUISM Security Control: 1211 NZISM 6.3 NIST 800-171 3.4.3 NIST 800-171 3.4.4 NIST 800-53 CM-3(2) NIST 800-53 CA-1 NIST 800-53 SA-1

1.2.8 Security | Plans and Quality (continued...)

#	Question	Tier	Response Options	Standard

Q4	Does your organisation have a documented and implemented security, privacy and online safety risk management framework and supporting processes, which outlines at a minimum:
	• Scope and categorization of information assets and systems;
	• Periodic or continuous assessment of risks/ threats, including those relating to the supply chain (e.g. from outsourced services that the solution relies on);
	• Selected and implemented controls to manage risks with the following details recorded in a risk register:
	  • Identified security risks, categories and risk ratings;
	  • Risk owner(s);
	  • Mitigation actions;
	  • Accepted risks (where applicable) and;
	  • Residual risk ratings after implementing mitigation actions
	• Proactive monitoring and testing of information assets and systems to maintain the security posture on an ongoing basis
	• the framework is to be reviewed regularly and in response to security incidents?
		1 & 2	A. No - none of the above
			B. Yes - some of the above
			C. Yes - all of the above (T1, T2)
				AUISM Security Control: 1636, revision 0, ISM Security Control: 1526, revision 1
				NZISM 3.2.10-13
				NZISM 3.3.5-8
				NZISM 4.1
				NIST 800-171 3.11.1
				NIST 800-53 RA-1
				NIST 800-53 CA-1
				NIST 800-53 SC-1

Q5	Are all service application developments assessed as per a security testing methodology that is consistent with the guidance provided by the latest industry standard frameworks (e.g., Open Web Application Security Project (OWASP) Testing Guide v4.2, Building Security In Maturity Model (BSIMM))?	1 & 2	A. No (#T1, #T2) B. Yes - security testing partially satisfies the guidance provided in an industry standard framework (please specify framework) C. Yes - security testing fully satisfies the guidance provided in an industry standard framework (T1, T2) (please specify framework)	AUISM Security Control: 1239 NZISM 14.4.6 NZISM 14.5.8 NIST 800-53 SA-10

1.2.8 Security | Plans and Quality (continued...)

#	Question	Tier	Response Options	Standard
Q6	Does your organisation have a documented and implemented IT Asset management process including: • A register of all components that make up the service, including software, databases, middleware, infrastructure etc (their version numbers, patch levels, configuration, network address (if static), hardware address, machine name, asset owner, asset department, approval for connecting to the organisation's network. For software the publisher, installation date, business purpose, URI, deployment mechanism, decommission date); • An ICT equipment and media register that is maintained and regularly audited; • A directive that ICT equipment and media are secured when not in use; • The secure disposal of ICT equipment and media (including sanitizing / removal of any data or secure destruction / shredding); • A register of all baseline configurations associated with components, that is updated in line with the organisation's system hardening process, with each component tracked only once. • Documentation of security and privacy impacts of asset changes; and • Removal, denial of access or the quarantining of any identified unauthorized assets on a regular basis.	1	A. No - none of the above B. Yes - some of the above C. Yes - all of the above (T1, T2)	AUISM Security Control: 0336, revision 4, ISM Security Control: 1713, revision 1 NZISM 8.4 NZISM 12.6 NZISM 13.4-13.6 NIST 800-171 3.4.1 NIST 800-53 CM-1 (DESIRABLE) NIST 800-53 CM-8 (DESIRABLE) NIST 800-53 CM-9 (DESIRABLE) NIST 800-171 3.8.3 NIST 800-53 SA-10 CIS 1.1, 1.2, 2.1,

1.2.8 Security | Plans and Quality (continued...)

#	Question	Tier	Response Options	Standard
Q7	Does your organisation have a documented and implemented information security policy that outlines the following at a minimum: • management direction and support for information security; • requirement to comply with applicable laws and regulations; • information security roles and corresponding responsibilities / accountabilities; • access controls for sensitive information aligned to the information security roles; • how long security logs are retained for • Is the policy reviewed regularly and in response to security incidents? • which events are logged • policies relating to incident response, including a roadmap for an incident response capability if not already implemented • personnel security • physical and environmental protections • system boundaries, environments of operation, and relationships / connections to other systems; and • policies relating to preserving system and information integrity, including system monitoring	1 & 2	A. No B. Yes (T1, T2)	AUISM Security Control: 1478 revision 1. NZISM 5.1.7 NZISM 5.2 NIST 800-53 AC-1 NIST 800-171 3.3.1 NIST 800-171 3.3.3 NIST 800-53 AU-1 NIST 800-53 IR-1 (DESIRABLE) NIST 800-53 PS-1 NIST 800-53 PE-1 NIST 800-171 3.12.4 NIST 800-53 SI-1
Q7a	Does your organisation have a documented and implemented security training and awareness policy that outlines the following at a minimum: • management direction and support for information security; • requirement to comply with applicable laws and regulations; • security training and awareness processes to be adopted; • requirement for communication to management to ensure they maintain an awareness of, and focus on, addressing privacy and security issues? • requirement for communication to management to ensure they maintain an awareness of, and focus on, addressing privacy and security issues? • Is the policy reviewed regularly and in response to security incidents?	1 & 2	A. No B. Yes (T1, T2)	NIST 800-53 AT-1

1.2.8 Security | Plans and Quality (continued...)

#	Question	Tier	Response Options	Standard
Q7b	Does your organisation have a documented and implemented identification and authentication policy that outlines the following at a minimum: • management direction and support for identification and authentication; • requirement to comply with applicable laws and regulations; • policy on user identifiers; • policy on passwords and password updates; • policy on one-factor and multi-factor authentication security and usage; and • is the policy reviewed regularly and in response to security incidents?	1 & 2	A. No B. Yes (T1, T2)	NIST 800-53 IA-1 (DESIRABLE)
Q7c	Does your organisation have a documented and implemented maintenance policy that outlines the following at a minimum: • management direction and support for maintenance; • requirement to comply with applicable laws and regulations; • governs the development of a maintenance plan for the organisation's software, hardware, and firmware; • ensures that any software no longer supported with updates is either removed as unauthorized, or else documented as an exception with mitigating controls and risk acceptance; • ensures that only fully supported web browsers and email clients are allowed to execute in the enterprise; • is the policy reviewed regularly and in response to security incidents?	1 & 2	A. No B. Yes (T1, T2)	NIST 800-53 MA-1 CIS 2.2, 2.3, 9.1
Q7e	Does your organisation have a documented and implemented security planning policy that outlines the following at a minimum: • management direction and support for planning around security; • requirement to comply with applicable laws and regulations; • policy that governs the development of security-related plans in the organisation overall? • requires coordination around the plans with other business units within the organisation as appropriate?; and • is the policy reviewed regularly and in response to security incidents?	1 & 2	A. No B. Yes (T1, T2)	NIST 800-53 PL-1 NIST 800-53 PL-2(3) (DESIRABLE)

1.2.8 Security | Plans and Quality (continued...)

#	Question	Tier	Response Options	Standard
Q7e	Does your organisation have a documented and implemented systems and services acquisition policy that outlines the following at a minimum: • management direction and support for planning around systems and services acquisition; • requirement to comply with applicable laws and regulations; • policy that governs the acquisition of resources, including: security and privacy requirements and acceptance criteria; • requiring the developer of the system or service to provide: a description of the functional properties of any security controls; relevant design and implementation information for security controls; a listing of all functions, ports, protocols and services in use; conformance with NIST FIPS-201-3 for any Personal Identity Verification functionality (smart card or equivalent for access to premises) • requirement for administrator documentation covering addressing in configuration, use and maintenance, and known vulnerabilities; • requirement for user documentation covering security and privacy functionality they can access, secure user interaction, and user responsibilities; • logging of attempts to obtain documentation that have been unsuccessful; and • is the policy reviewed regularly and in response to security incidents?	1 & 2	A. No B. Yes (T1, T2)	NIST 800-53 SA-4 NIST 800-53 SA-4(1) NIST 800-53 SA-4(2) NIST 800-53 SA-4(9) NIST 800-53 SA-4(10) NIST 800-53 SA-5
Q7f	Does your organisation have a documented and implemented data management policy that outlines the following at a minimum: • Identification of data assets; • recording of data assets in a data inventory; • data asset ownership; • tracking of data sensitivity; • handling of data; • data retention limits; • disposal requirements informed by data sensitivity and retention standards; and • is reviewed and updated annually with a priority on sensitive data?	1 & 2	A. No B. Yes (T1, T2)	CIS 3.1, CIS 3.2

1.2.8 Security | Plans and Quality (continued...)

#	Question	Tier	Response Options	Standard
Q8	Does the service's application development have the following characteristics: • Environments are separated into at least development, testing and production environments; • Development and modification of software only takes place in development environments; • Unauthorized access to the authoritative software source is prevented; • Secure-by-design principles and secure programming practices are used as part of application development. (This includes: integrating the organisation's security and privacy risk management into application development; assigning responsibility for security and privacy as defined roles to individuals during application development); • Applies the National Institute for Standards and Technology (NIST)'s Secure Software Development Framework (SSDF) for all software development activities • Privacy-by-design principles; • Threat modelling is used in support of application development; and • Alignment to a security and privacy architecture that has been drawn up for the system	1 & 2	A. No – none of the above B. Yes - some of the above C. Yes - all of the above (T1, T2)	NZISM 14.4 NZISM 14.5 NIST 800-53 PL-8 NIST 800-171 3.13.2 NIST 800-53 SA-3

1.2.10 Security | Data Deletion and Retention

#	Question	Tier	Response Options	Standard
D1	Are all data backups stored for a minimum of 3 months?	1 & 2	A. No B. Yes (T1, T2)	AUISM Security Control: `1511 NZISM 6.4
D2	Is deletion of data from the service: • Performed securely commensurate with the data's sensitivity; • And certified?	1 & 2	A. No B. Yes, but certificate not provided to customer C. Yes, with certificate provided to customer upon request (T1)	NZISM 13.1 NZISM 13.4-13.6 NZISM 22.1.26 CIS 3.5
D3	Is the full restoration of backups tested at least once when initially implemented and each time major information technology infrastructure changes occur, or at least annually? (e.g., technology stack changes, vendor changes, platform changes)?	1 & 2	A. No (#T1, #T2) B. Yes (T1, T2)	AUISM Security Control: 1515 NZISM 6.4

1.2.10 Security | Data Deletion and Retention (continued...)

#	Question	Tier	Response Options	Standard
D4	Is the partial restoration of backups tested on a quarterly or more frequent basis?	1 & 2	A. No (#T1) B. Yes (T1, T2)	AUISM Security Control: 1515 NZISM 6.4
D5	Does the service have a documented and implemented data retention policy including: • Minimum data retention period; • Maximum data retention period; and • The deletion of identifying or sensitive data which is no longer required?	1 & 2	A. No B. Yes (T1, T2)	CIS 3.4

1.2.11 Security | Compliance Control

Criteria around organisation compliance with externally managed certifications and assessments relevant to security.

#	Question	Tier	Response Options	Standard
CC1	Select the compliance certifications or security assessments that have been completed for the service and your organisation, or another organisation contracted by you to perform the development, maintenance and/or support of your solution (excluding the infrastructure provider e.g., AWS, Azure, Sendgrid)	1 & 2	A. ISO/IEC27001 B. SOC 2 Type II C. FEDRAMP / StateRMP (NIST) D. IRAP F. Cloud Security Alliance STAR G. Cloud Vendor Assessment Tool (HECVAT or K12CVAT) H. UK Cyber Essentials I. None of the above	NZISM 5.8 NZ PSR – INFOSEC3, GOV8 NIST 800-171 3.12.1
CC1a	Which compliance certifications or assessments do you complete on a regular basis (i.e. repeatedly)?	1 & 2	(Please specify)	NIST 800-171 3.12.1
CC1b	Which compliance certifications or assessments are undertaken by independent assessors?	1 & 2	(Please specify)	NIST 800-171 3.12.1
CC1c	Select the privacy related compliance certifications or assessments that have been completed for the service and your organisation, or another organisation contracted by you to perform the development, maintenance and/or support of your solution (excluding the infrastructure provider e.g., AWS, Azure, Sendgrid)	1 & 2	A. Privacy confirmation (GDPR, SOPAA) B. SOPIPA C. Other (please specify) D. None of the above	NIST 800-53 CA-2(1) NIST 800-53 CA-7(1)

1.2.11 Security | Compliance Control (continued...)

#	Question	Tier	Response Options	Standard
CC2	If the solution processes electronic payments or holds credit card data is it Payment Card Industry Data Security Standards (PCI DSS) compliant?	1 & 2	A. No (#T1, #T2) B. Yes – service is PCI compliant (T1, T2) C. Yes – outsourced to PCI compliant third party (please specify) (T1, T2) D. N/A – Solution does not process payments or hold credit card data (T1, T2)	NZISM 5.8

1.2.12 Security | Governance

Criteria around how security is resourced and managed within the organisation.

#	Question	Tier	Response Options	Standard
G01	Is there a nominated role within the organisation responsible for information security (i.e., CIO, CTO, CISO)?	1 & 2	A. No B. Yes (T1, T2) (Please specify role title)	AUISM 0714 NZISM 3.2
G02	Is there a nominated role within the organisation responsible for privacy (i.e., CIO, CTO, CISO, Privacy Officer, Data Protection Officer,)?	1 & 2	A. No B. Yes (T1, T2) (Please specify role title).	NZPP
G03	Has responsibility for and ownership and account-ability of critical system assets been assigned to individual/s in the organisation?	1 & 2	A. No B. Yes (T1, T2)	NZISM 3.4
GO3a	Are security and privacy requirements factored into the organisation's planning and budget and is there a discrete line item in the budget for security and privacy?	1 & 2	A. No B. Yes (T1, T2)	NIST 800-53 SA-2
G04	What countries are your organisation's security and privacy operations teams and real-time monitoring and incident response systems located?	1 & 2	A. Entirely within Australia and/or New Zealand (please specify) (T1, T2) B. From other countries (please specify country/s) C. No defined security and privacy operations teams	

1.3 Criteria | Privacy

Criteria relevant to the assessment of the software product for privacy, as distinct from security or interoperability.

#	Question	Tier	Response Options	Standard
PA1	Are the terms of service/use and/or data processing agreement made available free of charge, and, published on the internet or provided to customers prior to use of the service?	1 & 2	A. No B. Yes (T1, T2)	NIST 800-171 3.1.9 (DESIRABLE)
PA2	As per the terms of service, what, if any, age restrictions apply to the use of the service?	1 & 2	A. Users must be over a certain age (please specify) B. Users under a specified age can use the service with parent/guardian consent (please specify) C. No age restrictions apply (T1, T2) D. Other (please specify) E. NA - this service will not be used by students (T1, T2)	
PA3	What are the specified definitions of intellectual property ownership, including copyright, in the terms of use for the service? (e.g., user generated content)? Include excerpt from terms of use.	1 & 2	A. Not specified B. Service provider has ownership or unrestricted license to copy, alter, distribute, perform, display to all other users, third parties, affiliated organisations, etc. The service provider notifies users if their intellectual property is used for any of these purposes. C. Service provider has ownership or unrestricted license to copy, alter, distribute, perform, display to all other users, third parties, affiliated organisations etc. The service provider does not notify users if their intellectual property is used for any of these purposes. D. User retains intellectual property rights to their own work created within and/or uploaded to the service (T1, T2)	
PA4	As per the terms of service, are users forewarned in the event the service provider wishes to terminate their account?	1 & 2	A. No B. Yes (T1, T2) C. N/A - Service provider does not terminate accounts (T1, T2)	

1.3.2 Criteria | Privacy Requests

Criteria around how the software product requests potentially sensitive information from users, and what information it requests.

#	Question	Tier	Response Options	Standard
PR1	Is the privacy policy made available free of charge, stating explicitly what sites and services it covers, and: • Published on the internet; or • Provided to customers prior to use of the service?	1 & 2	A. No (#T1, #T2) B. Yes (T1, T2)	APP: 1.5 NZPP-3 NIST 800-171 3.1.9 (DESIRABLE)
PR1A	Enter the URL for the service's Privacy Policy/Data Processing Agreement or upload the Privacy Policy document	1 & 2		NZPP-3
	Does the privacy policy for the service outline the following requirements about the collection and management of personal information at a minimum: • The kinds of personal information that the entity collects and holds; • How the entity collects and holds personal information; • The purposes for which the entity collects, holds, uses and discloses personal information; • How an individual may access personal information about the individual that is held by the entity and seek the correction of such information; • How an individual may complain about a breach of their privacy, and how the entity will deal with such a complaint; • Whether the entity is likely to disclose personal information to overseas recipients; and • If the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy?			

1.3.2 Criteria | Privacy Requests (continued...)

#	Question	Tier	Response Options	Standard
PR2	Does the privacy policy for the service outline the following requirements about the collection and management of personal information at a minimum: • The kinds of personal information that the entity collects and holds; • How the entity collects and holds personal information; • The purposes for which the entity collects, holds, uses and discloses personal information; • How an individual may access personal information about the individual that is held by the entity and seek the correction of such information; • How an individual may complain about a breach of their privacy, and how the entity will deal with such a complaint; • Whether the entity is likely to disclose personal information to overseas recipients; and • If the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy?	1 & 2	A. No (#T1, #T2) B. Yes - includes some of the above (#T1, #T2) C. Yes - includes all of the above (T1, T2)	APP: 1.4 NZPP-3 NZPP-6 NZPP-7
PR3O	Are user accounts generated centrally, or by end users?	1 & 2		
PR3A	What mandatory information is collected by the service when school staff generate their own accounts for this service? Select all that apply. If not required, select N/A.	1 & 2	A. Title B. First name C. Surname D. Email address E. Gender F. Date of birth (i.e., dd/mm/yy) G. Age, month and year of birth, or year of birth H. Year level I. Country or state/province J. Role (for school leaders) K. Evidence of identity (e.g. driver's license) L. Other (please specify): M. N/A - school staff do not register their own accounts for this service	NZPP-3

1.3.2 Criteria | Privacy Requests (continued...)

#	Question	Tier	Response Options	Standard
PR3B	What mandatory information is collected by the service when students generate their own accounts for this service? Select all that apply. If not required, select N/A.	1 & 2	A. Title B. First name C. Surname D. Email address E. Gender F. Date of birth (i.e., dd/mm/yy) G. Age, month and year of birth, or year of birth H. Year level I. Country or state/province J. Role (for school leaders) K. Evidence of identity L. Other (please specify): M. N/A - students do not register accounts for this service N. N/A - students do not register their own accounts for this service	NZPP-3
PR3C	What mandatory information is collected by the service when parents generate their own accounts for this service? Select all that apply. If not required, select N/A. *NOTE: This question relates to when parent accounts are required for school use of the service. If parent accounts are not required, select, "N/A parent accounts are not required for school use of this service".*	1 & 2	A. Title B. First name C. Surname D. Email address E. Gender F. Date of birth (i.e., dd/mm/yy) G. Age, month and year of birth, or year of birth H. Year level I. Country or state/province J. Evidence of identity K. Other (please specify): L. N/A - parent accounts are not required for school use of this service M. N/A - parents do not register their own accounts for this service	NZPP-3

1.3.2 Criteria | Privacy Requests (continued...)

#	Question	Tier	Response Options	Standard
PR4A	What mandatory information is collected by the service when a school-based administrator (or the service) generates accounts on behalf of school staff? Select all that apply. If not required, select N/A.	1 & 2	A. Title B. First name C. Surname D. Email address E. Gender F. Date of birth (i.e., dd/mm/yy) G. Age, month and year of birth, or year of birth H. Year level I. Country or state/province J. Evidence of identity K. Other (please specify): L. N/A - school-based administrators or teachers or the service provider cannot generate accounts on behalf of staff	NZPP-3
PR4B	What mandatory information is collected by the service when a school-based administrator (or the service) generates accounts on behalf of students? Select all that apply. If not required, select N/A.	1 & 2	A. Title B. First name C. Surname D. Email address E. Gender F. Date of birth (i.e., dd/mm/yy) G. Age, month and year of birth, or year of birth H. Year level I. Country or state/province J. Evidence of identity K. Other (please specify): L. N/A - school based-administrators, teachers or the service provider cannot generate accounts on behalf of students	
PR4C	What mandatory information is collected by the service when a school-based administrator (or the service) generates accounts on behalf of parents? Select all that apply. If not required, select N/A.	1 & 2	A. Title B. First name C. Surname D. Email address E. Gender F. Date of birth (i.e., dd/mm/yy) G. Age, month and year of birth, or year of birth H. Year level I. Country or state/province J. Evidence of identity K. Other (please specify): L. N/A - school based-administrators, teachers or the service provider cannot generate accounts on behalf of parents	

1.3.2 Criteria | Privacy Requests (continued...)

#	Question	Tier	Response Options	Standard
PR5	Do the terms of use for the service require complete and accurate information to be entered when registering accounts for the service (e.g., are the use of pseudonyms or de-identified information not permitted)? Please include excerpt(s) from the terms of service.	1 & 2	A. Yes (please include excerpt from the terms of service) B. No (T1, T2)	
PR6	Are customers/users offered anonymity and/or pseudonymity when dealing with the service provider in some circumstances (e.g., providing feedback)?	1 & 2	A. No B. Yes, please specify circumstances (T1, T2)	APP: 2.1 NZPP-1
PR7	Are mandatory fields clearly distinguished from optional fields during the standard account registration process?	1 & 2	A. No B. Yes (T1, T2)	NZPP-3
PR8	Are mandatory fields clearly distinguished from optional fields when schools, teachers, or the service register accounts on behalf of other users (e.g., students, staff, or parents)?	1 & 2	A. No B. Yes (T1, T2)	NZPP-3
PR9	If unsolicited personal information is provided to the service (e.g., when existing customer data is uploaded to the service), is the information destroyed or de-identified as soon as practicable if it is lawful to do so?	1 & 2		NZPP-9

1.3.2 Criteria | Privacy Requests (continued...)

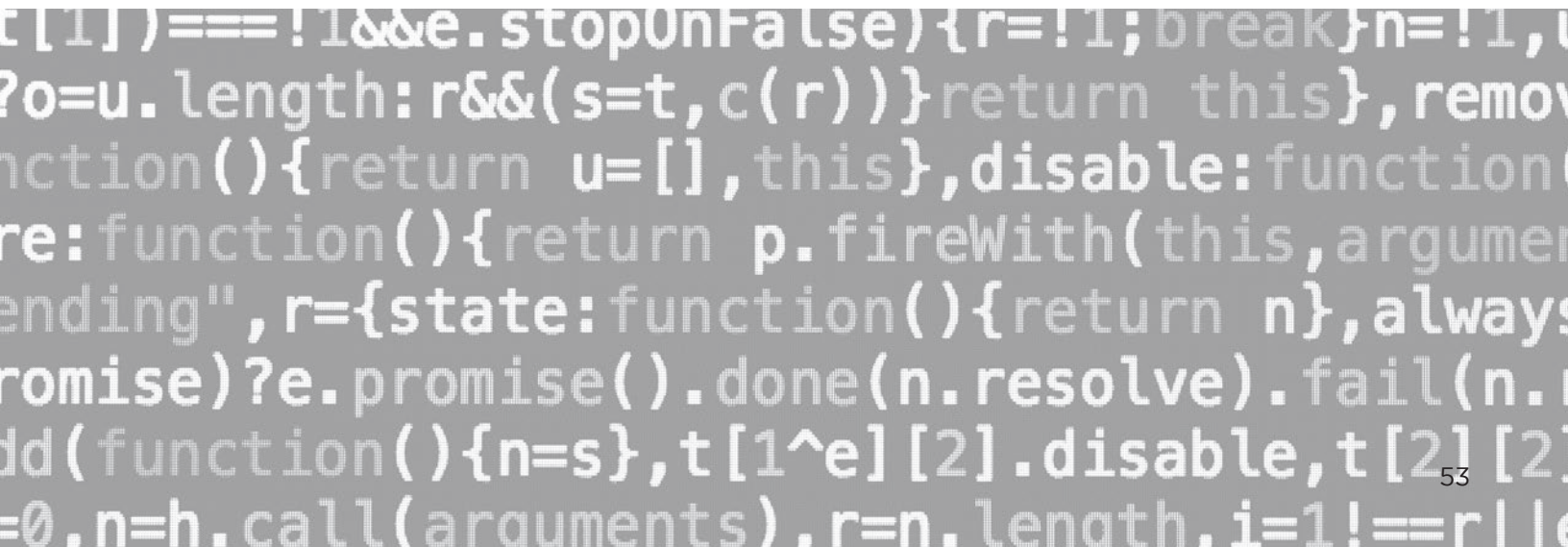
#	Question	Tier	Response Options	Standard
PR10	Does your organisation share user data with third parties in any circumstance other than the following? If yes, please specify. • the individual has consented to the use or disclosure of the information; • the use or disclosure of the information is required or authorized by or under a law or a court/tribunal order in the customer's country; • the use or disclosure is required or permitted under privacy legislation in the customer's country; or • the entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body? For service in Australia, refer to the Australian Privacy Principles, as well as the permitted general situations and permitted health situations. For service in New Zealand, refer to the Privacy Principles and information sharing provisions in the Privacy Act 2020, as well as the Oranga Tamariki Act 1989 and the Family Violence Act 2018. For the UK, refer to Keeping Children Safe in Education	1 & 2	A. Yes (please specify) (#T1, #T2) B. Yes - however the user must consent to the use or disclosure of information (create new risk on assessment report) C. No (T1, T2)	APP: 6.1, 6.2 NZPP-11 NIST 800-171 3.1.22
PR11	Is subscription to the service's commercial mailing list opt-in by choice *Commercial mailing lists are those that are used for the purpose of distributing sales and marketing and promotional materials, including (but not limited to) competitions, education research related to the product, and end user feedback.* *Commercial mailing lists do not include lists used for the purpose of sending important service information, such as notifications of service disruption, data breach or loss; upgrade notifications; and subscription renewals.*	1 & 2	A. Users cannot opt-out of the service's commercial mailing list B. No, users are automatically subscribed but can opt-out after the fact C. Yes, users can choose to opt-in to subscriptions (T1, T2) D. N/A - no commercial mailing list (T1, T2)	

1.3.2 Criteria | Privacy Requests (continued...)

#	Question	Tier	Response Options	Standard
PR12	Does the service adopt government related identifiers of individuals as its own identifier of the individual or use or disclose government related identifiers for any reasons other than the list below: • The government related identifier is required or authorized by or under a law or a court/tribunal order within the customer's country; • Use or disclosure is necessary for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions; • Use or disclosure is necessary for the organisation to fulfill its obligations to a government agency or education authority within the customer's country; • Use or disclosure is required or authorized by or under a law or a court/tribunal order within the customer's country; • The organisation reasonably believes the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities; • The identifier, organisation or circumstances are prescribed by regulations?	1 & 2	A. Yes (provide details of the identifier(s) and how each is used) (#T1, #T2) B. No (T1, T2)	APP: 9.1, 9.2 NZPP-13
PR13	Does your organisation and/or product have a process or provide a facility which allows customers/schools to provide end-users (staff, students, parents) with the ability to correct, request access to, or request deletion (where applicable) of their personal information/data?	1 & 2	A. No (#T1, #T2) B. Yes - with a cost and resolved outside of 3 months C. Yes - with a cost and resolved within 3 months D. Yes - free of charge and resolved outside of 3 months (T2) E. Yes - free of charge and resolved within 3 months (T1, T2) F. NA - service does not collect personal information (T1, T2)	APP: 12.1, 13.1 NZPP-6 NZPP-7

1.3.2 Criteria | Privacy Requests (continued...)

#	Question	Tier	Response Options	Standard
PR14	Does the service provide any discovery functionality which allows users from one school to find, access or discover users or personal information from another school, or organisation? Examples include enabled searching (by user, user details or resources), or data sharing (e.g. to support student transfer) or integration (e.g. for analytics) between customers (e.g. different schools). Select all that apply.		A. No discovery functionality exists within service (T1,T2) B. Discovery functionality can be restricted to the user's current school/year level/class C. Discovery functionality is disabled by default D. An administrator can restrict discovery functionality at the user level (i.e. allow some but not all users access discovery functionality) E. Discovery is possible, but none of the controls above are available (#T1, #T2)	NZPP-11
PR15	Does the service capture a user's location data?		A. No, user location data not required. (T1, T2) B. The service must capture user location data to function. Location data is captured with a user's explicit consent (T1, T2) C. The service must capture user location data to function. Location data is captured without a user's explicit consent. D. The service does not require user location data to function, but does capture it with a user's explicit consent. E. The service does not require user location data to function, but does capture it without a user's explicit consent.	



1.3.3 Criteria | Functionality

Criteria around what functionality within the software product could potentially compromise user privacy.

Please note: Functionality questions allow us to better understand how given functionality works and what controls are available. Generally speaking, an ability to disable, restrict access to, or moderate functionality will result in a lower risk level.

#	Question	Tier	Response Options	Standard
PF1	When using the service, are users under the age of 18 exposed to advertising and/or offers?	All	A. Yes B. No (T1, T2)	
PF2	Does the service provide functionality that allows school-based administrator accounts to control role-based access for school users (e.g., staff or students) in order to restrict access to stored information and/or functionality within the system?	1 & 2	A. No B. Yes, please provide details (T1, T2) C. N/A (T1, T2)	UKCE A7.1 - 7.4
PF3	Does the registration of an account or use of the service generate a user 'profile' within the service, and if so, can visibility be restricted (e.g., made private or restricted to known users)?	1 & 2	A. Profile is generated, but user or administrator cannot restrict visibility of their profile B. Profile is generated, and user or administrator can restrict visibility of their profile C. Profile is generated but only visible to user (e.g., visibility is restricted by default) (T1, T2) D. No user profile is generated (T1, T2) Informational only, used to generate subsequent questions.	

1.3.3 Criteria | Functionality (continued...)

#	Question	Tier	Response Options	Standard
PF4	Select all functionality available within the service.	All	Informational only, used to generate subsequent questions. A. Forms, surveys and eSignatures B. Online meetings, video conferencing, audio conferencing C. Remote access tools D. Screen Sharing E. Chat / Instant Messaging F. Commenting and communities / forums G. Quiz, poll, flashcard creation and/or distribution H. File download, including executable, developer tools, images etc. I. Direct email J. File upload and storage, and file sharing and collaboration K. Content creation and collaboration L. Content libraries M. Notifications and alerts N. Online learning activities, assessments and/or games O. Administrative support services and records management P. Data integration, aggregation, data broker, data hub, data distribution hub Q. Assessment or collection of health and well-being information including socio-emotional factors (e.g., physical and mental health, well-being, behavior) R. Other S. None of the above	
PF5	In relation to the form, survey and/or eSignature functionality, select which features are offered within the service. Select all that apply.	All	A. Online forms - service provider generated, non-editable B. Online forms - customizable / editable / user generated C. Surveys - service provider generated, non-editable D. Surveys - customizable / editable / user generated E. eSignatures F. Forms/surveys can be distributed and/or shared via linked social media accounts (Facebook, Twitter, etc.) G. Forms/surveys can be shared as templates for re-use by others	

1.3.3 Criteria | Functionality (continued...)

#	Question	Tier	Response Options	Standard
PF6	In relation to the online meeting, video conference, audio conferencing and/or livestreaming functionality available within the service, select all that apply.		A. Access to sessions can be made available to the public B. Access to sessions can be made private (e.g., access to sessions is invitation only) C. Participant details can be displayed to all session participants D. Participants can be displayed with de-identified/anonymous details or kept private E. Sessions can be recorded and made available to the public F. Sessions can be recorded and made private (e.g., participants only) G. Audit logs are not kept for all recordings (#T1, #T2) H. Participants are not notified if they are participating in a recorded session (e.g., via on screen prompt) (#T1, #T2)	NIST 800-171 3.13.12 NIST 800-171 3.13.14
PF7	In relation to the remote access tools available within the service, select all that apply.		A. Remote access tools can be disabled by an administrator or moderator B. Remote access sessions can be initiated without the agreement of the user (#T1, #T2) C. Users cannot take back control during remote access sessions (#T1, #T2) D. Users cannot terminate remote access sessions once initiated (#T1, #T2) E. Onscreen notification is displayed throughout remote access sessions F. Remote access sessions are not logged (#T1, #T2) G. Remote access sessions are not audited by your organisation to ensure appropriate, authorized access	NIST 800-171 3.1.12 (DESIRABLE) NIST 800-171 3.13.12 NIST 800-171 3.13.14
PF8	In relation to the screen sharing functionality available within the service, select all that apply.		A. Use of screen sharing functionality is disabled by default B. Screen sharing can be disabled by an administrator or moderator C. Screen sharing sessions are initiated and/or accepted by the user who is sharing their screen D. Screen sharing sessions are not logged (#T1, #T2)	

1.3.3 Criteria | Functionality (continued...)

#	Question	Tier	Response Options	Standard
PF9	In relation to the chat/instant messaging functionality available within the service, select all that apply.		A. Chat/instant messaging is unmoderated B. The service moderates chat/messages using a profanity filter C. The service moderates chat/instant messaging and reserves the right to remove posts and/or users that breach the Terms of Use D. Users can report chat/instant messaging that breaches the Terms of Use E. Users can chat/message with non-account holders (i.e., no log in is required to participate in chat/messaging) F. Communication can be limited to restricted groups only (e.g., class, year level) G. Chat/instant messaging can be disabled by an administrator/moderator H. Chat/instant messaging is visible to an administrator (e.g., teacher) in real time I. Chat/instant messaging is not logged (#T1, #T2) J. None of the above	NIST 800-171 3.1.12 (DESIRABLE) NIST 800-171 3.13.12 NIST 800-171 3.13.14
PF10	In relation to the commenting and communities/forums functionality available within the service, select all that apply:		A. Non-account holders can post comments (i.e., no log in is required to participate in commenting) B. The service applies a profanity filter prior to publishing C. The service moderates comments and reserves the right to remove posts and/or users that breach the Terms of Use D. Users can report comments that breach the service's Terms of Use E. Comments must be approved by an administrator or the service prior to publishing F. Commenting can be disabled by an administrator/moderator G. An administrator can control what users can comment on and which users can comment (e.g., a teacher can restrict students to only comment on the work of classmates) H. Commenting is unmoderated I. Comments are not logged (#T1, #T2) J. Users can upload files or share projects or files in forums/communities K. None of the above	

1.3.3 Criteria | Functionality (continued...)

#	Question	Tier	Response Options	Standard
PF11	In relation to the quiz, poll and flashcard functionality, select which features are offered within the service. Select all that apply.		A. Quizzes - service provider generated, non-editable B. Polls - service provider generated, non-editable C. Flashcards - service provider generated, non-editable D. Quizzes - customizable / user generated E. Polls - customizable / user generated F. Flashcards - customizable / user generated G. Quizzes, polls and/or flashcards can be shared as templates for re-use by others	
PF13	In relation to the file download functionality available, select all files types that can be downloaded within the service.		A. Executable files and/or code (e.g., .exe) B. Desktop publishing files (e.g., .doc, .pdf, .ppt) C. Image files (e.g., .png, .jpg, .jpeg) D. Audio files (e.g., .mp3, .wma, .wav) E. Video files (e.g., .avi, .mov, .wmv, .gif) F. Database files (e.g., .dat, .csv, .log, .mdb) G. Other	
PF14	At a minimum, are the following features built into the file download functionality available within the service: • All files are scanned for Malware/Viruses during download; • All files are scanned for Malware/Viruses while at rest; and • All files found to contain Malware/Viruses are deleted or quarantined?		A. None of the above (#T1, #T2, if also support download of .exe (A) or database files (F) from PF13) B. None of the above, but users cannot download files uploaded by other users C. Yes, some of the above D Yes, all of the above (T1, T2)	AUISM Security control: 0657 NZISM 14.1 NIST 800-171 3.14.2
PF15	When sending correspondence via the service on behalf of the school, how does the service send email communication to the school's recipients/audience? Select all that apply.		A. Sent from the school user's registered email address B. Sent from the service's domain (e.g., user@servicename.com) C. Sent from unverified, anonymous or invalid email addresses D. Other	

1.3.3 Criteria | Functionality (continued...)

#	Question	Tier	Response Options	Standard
PF16	What, if any, third party products are used to provide the file upload and storage functionality within the service? Select all that apply.		A. YouTube B. Vimeo C. Flickr D. Image Shack E. Picasa F. Other image and video streaming services G. DropBox H. Google Drive I. OneDrive J. Box K. iCloud L. Other cloud storage and file sharing M. No third-party products are used	
PF17	In relation to the file upload and sharing functionality available within the service, select all that apply.		A. Authors have control over who can view and/or edit their files B. Administrators (e.g., teachers) can restrict who can view and/or edit users' files C. Administrators can disable file sharing D. None of the above E. Not applicable – file sharing is not supported	
PF18	At a minimum, are the following features built into the file upload functionality available within the service? • All files are scanned for Malware/Viruses during upload • All files are scanned for Malware/Viruses while at rest • All files found to contain Malware/Viruses are quarantined or deleted		A. None of the above (#T1, #T2) B. Yes, some of the above C. Yes, all of the above (T1, T2)	AUISM Security control: 0657 NZISM 14.1 NIST 800-171 3.14.2
PF19	In relation to the content creation functionality available within the service, select all that apply.		A. Users can share their content (e.g., via direct urls) B. Users have control over who can view or edit their content C. Administrators can restrict who can view and/or edit users' content D. Administrators can disable sharing of users' content E. None of the above	

1.3.3 Criteria | Functionality (continued...)

#	Question	Tier	Response Options	Standard
PF20	Select the response option which best describes the publication of user generated content. Publication means visible to all members and/or visitors to the service.		A. User generated content can be published to the service but no privacy settings can be applied B. User generated content can be published to the service and privacy settings can be applied C. User generated content cannot be published to the service	
PF21	In relation to the content libraries available within the service, select all that apply. Content may include:		A. Educational or curriculum aligned content and activities B. Non-educational content and activities C. Template libraries (e.g., presentations, web design, surveys etc.) D. Image, video and audio libraries E. Search results that are not filtered based on user characteristics (e.g., age, year level, user type etc.) F. None of the above	
PF22	Who can publish content to content libraries within this service (i.e., users or service provider); and is content subject to moderation to ensure users are not exposed to information, including images, video, text and/or recordings, which may be deemed: • Offensive by a reasonable member of the school community (e.g., nudity, pornography, graphic content, profanity, racist, sexist etc. and/or • Inappropriate for users under 18 years? Moderation may include: • The service reserves the right to remove content that breaches the Terms of Use • The service applies a profanity filter • The service has an implemented assurance procedure to ensure content conforms to quality standards prior to publication • Users can report content that breaches the Terms of Use Select all that apply.		A. Service provider generated content with moderation B. Service provider generated content without moderation C. User generated content with moderation D. User generated content without moderation	

1.3.3 Criteria | Functionality (continued...)

#	Question	Tier	Response Options	Standard
PF23	In relation to the notification and alert functionality available within the service, select all that apply.		A. Notifications and alerts can be one-way (broadcast) B. Notifications and alerts can be two-way e.g., parents/recipients can respond to notifications and alerts C. Notifications can be via email D. Notifications can be via SMS E. Notifications can be via push notifications F. Notifications and alerts can be disabled by an administrator/moderator G. For each notification and/or alert, the school and/or users can specify and/or limit the audience H. The school and/or user can create and manage a subscriber group, and only members of this group can receive notifications and/or alerts from the school and/or user	
PF24	Question removed from 2021.1			
PF25	In relation to the online learning activities, assessment and/or game functionality available within the service, select all that apply.		A. The service provides standardized testing B. The teacher or user can create their own online learning activities and/or games. C. Answers can include pre-defined response options (e.g., multiple choice, Likert scales etc.) D. Answers are numerical free text fields (e.g., 0-9) E. Answers are short response free text fields (e.g., typing, equations, units of measurement, spelling and vocabulary) F. Answers can include long response free text fields (e.g., sentences, paragraphs, essays etc.) G. Data analysis, analytics and/or reporting is generated H. Data analytics and/or reporting can be sent to parents via the service. I. Other	
PF26	Select the response option which best describes the publication of results on the service. Results are considered to be published if they are visible to anyone other than the owner of the results.		A. Student results can be published on the service but privacy settings cannot be applied. B. Student results can be published on the service and privacy settings can be applied. C. Student results cannot be published.	

1.3.3 Criteria | Functionality (continued...)

#	Question	Tier	Response Options	Standard
PF27	In relation to any other functionality that is offered by the service, select all that apply.		A. Online ordering B. Financial management or payment processing systems C. Enrollment management D. Student information, student management system, school administration or student administration system E. Customer relationship management F. Ticketing systems G. Electronic document and records management systems H. Data integration, aggregation, data broker, data hub, data distribution hub I. Library Management J. Visitor Management K. Event management, bookings, online ordering or fundraising L. Subject selection M. Class formation N. Assignment submission O. Plagiarism detection P. Roll marking Q. Absence reporting and notifications R. Timetabling S. Academic reporting T. Other U. None of the above	
PF28	What names do you, as the service provider, give to the various modules available within the service?		*Informational question- used to inform QA and data assets disclosed to service.*	

1.3.3 Criteria | Functionality (continued...)

#	Question	Tier	Response Options	Standard
PF29	What additional student data - other than that which is mandatory to register an account - can be provided to / collected by the service when used for its intended purpose? Please indicate whether this data field is mandatory or optional.		For each indicate mandatory, optional or not collected: A. Protection details B. Legal custodian arrangements C. Out of home care status D. Records of behavior incidents E. Behavioral observations/notes F. Support arrangements G. Professional case notes H. Consent I. Attendance, including reason for absence J. Records of interview and/or contact K. Academic results L. Academic testing M. Personality profiling, career goals and/or interests N. Unique Student Identifier O. Timetabling P. Emergency contacts Q. Other R. None of the above For each indicate mandatory, optional or not collected:	

1.3.3 Criteria | Functionality (continued...)

#	Question	Tier	Response Options	Standard
PF30	What additional student, staff and/or parent data - other than that which is mandatory to register an account - can be provided to / collected by the service when used by the school for its intended purpose? This question is not intended to collect information about parent's personal use of the service (e.g., when it is not associated with school use/subscription). For each data asset, please specify whether it relates to student, staff, or parent. Select N/A if not collected.		For each indicate mandatory, optional or not collected: A. Medical details B. Well-being information C. Year level D. Class name E. School name F. Works G. Image H. Video or audio recording I. Email address J. First name K. Surname L. Date of Birth M. Age, month and year of birth, or year of birth N. Home address O. Phone number P. Identification documentation Q. Electronic signature R. Cultural and citizenship details, racial or ethnic origin S. Religion T. Gender U. Languages spoken V. Username - determined by the user W. Country or State/province X. Responses - online learning, surveys, forms Y. Resume, CV, applications, references Z. Certificates and accreditation AA. User location data AB. N/A	
PF31	What, if any, other data not listed above can be disclosed to or collected by the service if used for its intended purpose? Please specify if data relates to student, staff or parent and whether it is mandatory or optional.		Free text field (informational)	

1.3.3 Criteria | Functionality (continued...)

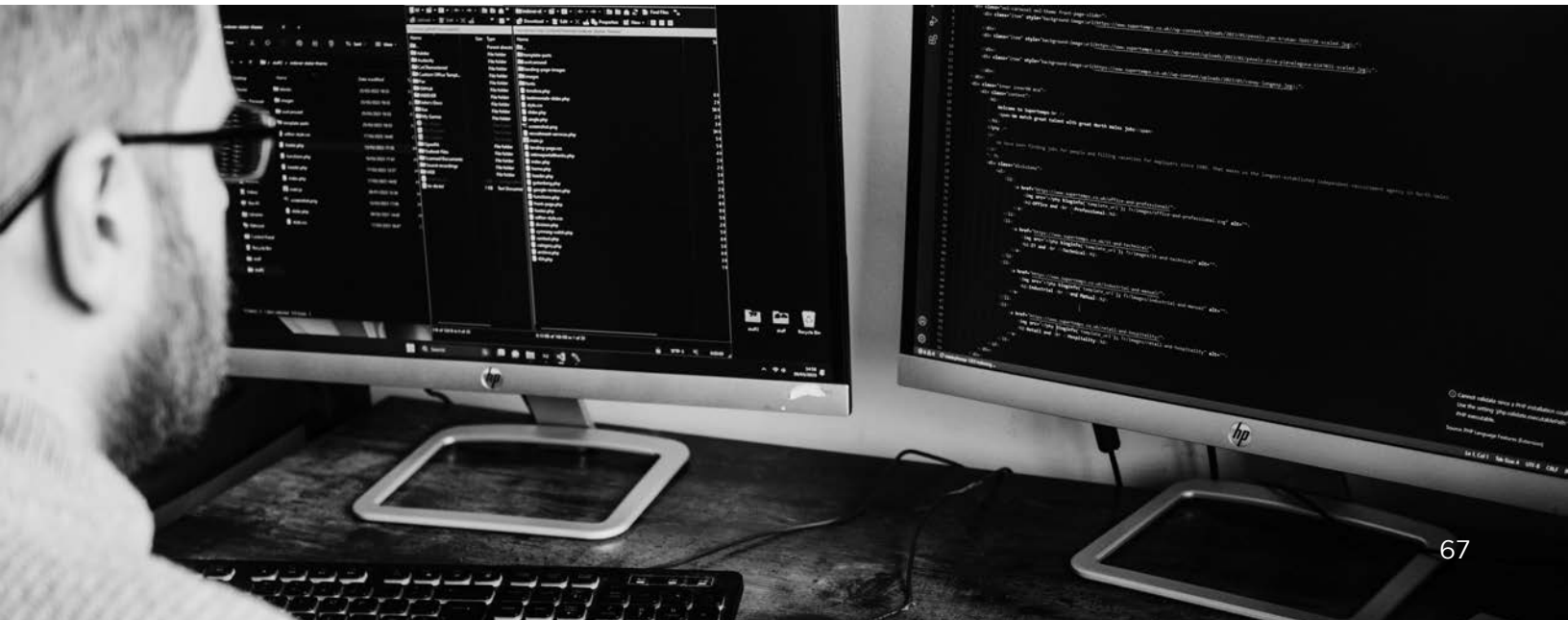
#	Question	Tier	Response Options	Standard
PF32	In relation to the data integration, aggregation, data broker, data hub, data distribution hub functionality, does the service (the collector of data/ data aggregator / data broker) assume ownership of any data transferred to, or transiting through, the service? In relation to the sharing of data with any third party (any service which receives data of any form from the service, including data aggregators and data hubs), are enforce-able, written agreements in place with data suppliers or recipients that covers: • the purpose for data sharing; • the scope of data to be shared (e.g., academic results); • the scale of data sharing (e.g., current student records only, or a specific year level); • the security and privacy controls in place in recipient systems; • ownership of data; • the interface characteris-tics of the exchange; • the sensitivity of the data being exchanged		A. Yes B. No (T1, T2)	NIST 800-53 CA-3
PF33	Furthermore, data agree-ments are updated to reflect changes in any of the above?		A. No B. Yes - Some of the above but data agreements not updated C. Yes - Some of the above with data agreements updated D. Yes (T1, T2)	NIST 800-53 CA-3

1.3.3 Criteria | Functionality (continued...)

#	Question	Tier	Response Options	Standard
PF34	Which security and privacy compliance certifications do recipient third party systems hold?		A. Industry standard security and privacy compliance certifications (e.g., ISO/IEC 27001/27002, ST4S, IRAP, etc.) (please specify) B. Other (please specify) C. None#	NIST 800-53 CA-3
PF35	Who authorizes the transfer of data, including the data scope (e.g., student academic results) and scale (e.g., only year 8 students) from the service (data integration / aggregation service, data broker, data hub, data distribution hub) to recipient third party systems:		Select all that apply: A. Data sharing can be controlled by the customer (school, school system or jurisdiction) (T1, T2) B. Data sharing can be controlled by the data aggregator (service being assessed) C. Data sharing can be controlled by the data recipient	
PF36	When a data breach or data loss event occurs in third party recipient systems, who notifies the customer (e.g., school, school jurisdiction or school system)?		A. Data aggregator notifies customer as soon as possible after discovery and provides all relevant details (T1, T2). B. Data aggregator notifies customer without commitment to timeframe and/or details not provided. C. Third party service notifies customer as soon as possible after discovery and provides all relevant details. D. Third party service notifies customer without commitment to timeframe and/or details not provided. E. Unknown (#T1, #T2) F. No notification of customer occurs (#T1, #T2)	

1.3.3 Criteria | Functionality (continued...)

#	Question	Tier	Response Options	Standard
PF37	In relation to the assessment or collection of health and well-being information through functionality available within the service, select all that apply:		A. Online forms – service provider generated, non-editable B. Surveys – service provider generated, non-editable C. Quizzes – service provider generated, non-editable D. Polls – service provider generated, non-editable E. Learning activities and/or game-based assessment F. Diagnostic and/or standardized testing G. Online forms – customizable / user generated H. Surveys – customizable / user generated I. Quizzes – customizable / user generated J. Polls – customizable / user generated K. Learning activities and/or game-based assessment – customizable / user generated N. Data analysis, analytics and/or reporting is generated for users based on their responses P. Well-being data analytics and/or reporting can be sent to parents via the service. Q. In-built monitoring and/or reporting tools identify respondents who may require follow-up or additional support. R. No in-built monitoring and/or reporting tools are provided to identify respondents who may require follow-up or additional support.	



1.3.3 Criteria | Functionality (continued...)

#	Question	Tier	Response Options	Standard
PF38	In relation to the assessment or collection of health and well-being information through functionality available within the service, select all that apply:		A. Responses can include pre-defined response options (e.g., multiple choice, Likert scales etc.) B. Responses are numerical free text fields (e.g., 0-9) C. Responses are short response free text fields (e.g., typing, equations, units of measurement, spelling, and vocabulary) D. Responses can include long response free text fields (e.g., sentences, paragraphs, essays etc.) E. Users can request further assistance or to talk to someone. F. Users can request further assistance or to talk to someone and this automatically notifies the school-nominated staff member. G. Users are de-identified and response data is aggregated/summarized so users and respondent data and reports are anonymous. H. Response data is aggregated / summarized so respondent data and reports do not identify the user. I. Respondent data and reports identify individuals for the purpose of monitoring, action and follow-up. J. Other	
PF39	With regards to personal information in the service, does the service log the following events: • Creation • Access • Modification • Deletion		A. No – None of the above B. Yes – Some of the above C. Yes – All of the above (T1, T2)	

1.5 Evidence

Depending on supplier responses to prior questions, the following documentary evidence is required to be uploaded (system accepts PDF, .DOC, .DOCX).

#	Evidence	Related to Question ID
EV1	Attestation of PCI-DSS Compliance	CC2
EV2	ISO27001 Certificate of Compliance / Statement of applicability	CC1
EV3	SOC 2 Type II Certification	CC1
EV4	FEDRAMP (NIST) Certification	CC1
EV5	IRAP Accreditation	CC1
EV6	Your organisation's Information Security Policy (external facing)	N/A
EV7	Business Continuity Plan as it relates to the service/s in question	Q2
EV8	Disaster Recovery Plan as it relates to the service/s in question	Q2
EV9	Incident Response Plan or Security Incident Management Plan	T6
EV10	Most recent penetration testing report (redacted) for the service/s in question	T1
EV11	Most recent vulnerability assessment reports (redacted) for the service/s in questions	T1
EV12	Patch management standards / process	T3, T4, T5
EV13	Your organisation's Secure Software Development Lifecycle process	Q5
EV14	Privacy compliance/certification	CC1
EV15	CSA Star	CC1
EV16	HECVAT	CC1
EV17	Sample agreement between service (data integrator, aggregator, data broker, data hub, data distribution hub) and third party	PF33
EV18	A list of all third-party services (company and service names) for which service accounts are required to be created (including access levels e.g., administrator, regular user)	A16A
EV19	Please supply a list of all third-party recipient services (company and service names) including the data types shared (e.g., personal information, medical information, financial data), and the purpose for sharing, with whom the service currently shares data.	PF32

1.6 Updates to the GESS Criteria, Response Options & Minimum Standards

Given the rapid change to the underlying standards which the GESS framework draws on, the GESS Team is estimating that the GESS framework (as represented in this document) will be updated every six to 12 months, with release likely occurring in January/February and June/July each year.

Appendix A | Tiers

Please note that the concept of 'Tiers' is currently a work in progress by the GESS group.

The breadth and depth of controls that should be applied to a supplier's service should be influenced by a number of factors. The GESS Team are currently considering three factors which would influence both the breadth and depth of controls that would apply to a service.

These factors are:

1. **Data:** The data stored or processed by the service.
2. **Functionality:** The service's functions.
3. **Reasonableness:** The service's display and communication of advertising or other materials which may cause offence.

For example, a service that handled sensitive student medical and emotional health and wellbeing data would be expected to encrypt data to a stronger degree and perhaps mandate multi factor authentication for all users, whereas a service that provided content repositories for teachers, consisting of various quality assured image libraries of the animals and automobiles would not require such stringent controls.

An exploration of what would influence tiers is included in the following tables.

Data Definitions	Data Examples
Sensitive information is a type of personal information that is given extra protection and must be treated with additional care. It includes any information or opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, or criminal record. It also includes health information and biometric information. Health information is a subset of sensitive information. It is any information or opinion about the health or disability of an individual, the individual's expressed wishes about the future provision of health services and a health service provided, currently or in the future, to an individual that is also personal information. Health information also includes personal information collected in the course of providing a health service. Financial information covers individual, family, staff, student financial records, bank details, debts, debt reminders etc. Identifiers cover government or other allocated identifiers which are possibly sensitive for the purposes of tracking an individual.	Sensitive information, including: **for students:** religion, birth certificate, language spoken at home, religious records (for example Baptism Certificate), religious education, whether Aboriginal or Torres Strait Islander, nationality, country of birth, legal information (custody, legal orders, out of home care), geographic location (GPS/lat/long), biometric data (eye/retinal imagery, fingerprints), welfare and discipline reports, passport details **for parents:** place of birth, religions, religious education, criminal record check, relevant child protection information (including working with children checks if volunteering to assist in the classroom), country of birth, whether Aboriginal or Torres Strait Islander, and nationality, legal information (custody, legal orders, out of home care), marital status / problems, voting in board elections **for job applicants, staff and contractors:** place of birth, religion, religious education, criminal record check, relevant child protection information (including working with children checks), member of professional associations, trade union membership, country of birth, nationality, OHS incident reports, staff complaints, workplace issue reports, letters of appointment/ complaint/ warning/ resignation, professional development appraisals, performance review, passport details **Health information, including:** • for students: medical background, immunization records, medical records, medical treatments, accident reports, absentee notes; medical certificates, health and weight, nutrition and dietary requirements, assessment results for vision, hearing and speech, reports of physical disabilities, illnesses, operations, pediatric medical, psychological, psychiatric, learning details (recipient special procedures), assessment for speech, occupational, hearing, sight, ADD, Educational Cognitive (IQ), health or other gov. service referrals • for parents: history of genetic and familial disorders (including learning disabilities), miscellaneous sensitive information contained in a doctor or health report; and • for job applicants, staff members and contractors: medical condition affecting ability to perform work, health information, medical certificates and compensation claims. **Financial information including:** Credit card details, account details, payment overdue notices, financial information relating to payment of school and administrative fees, banking details, scholarship details and information about outstanding fees, donation history, details of previous salary, salary being sought and other salary details, superannuation details **Identifiers includes:** local, state and federally or nationally assigned student, parent or staff identifiers (government related identifiers) *Examples:* Tax File Number, Victorian Student Number, Medicare number, Drivers License number, Passport, teacher registration number.

Data | Tier 2

Data Definitions	Data Examples
Personal information not captured in the 'High' tier: Personal information means information or an opinion about an identified individual or an individual who is reasonably identifiable whether the information is true or not, and whether the information is recorded in a material form or not. It includes all personal information regardless of its source. In other words, if the information or opinion identifies an individual or allows an individual to be identified it will be 'personal information' within the meaning of the Privacy Act. It can range from very detailed information, such as medical records, to other less obvious types of identifying information, such as an email address. Personal information does not include information that has been de-identified so that the individual is no longer identifiable	**for students:** name, sex/gender, physical address, email address, social media handles, phone number, date of birth (and age), conduct reports, next of kin details, emergency contact numbers, names of doctors, school reports and exam/test results, attendances, assessments, previous school history, referrals (e.g. government welfare agencies/departments), correspondence with parents, photos, current/previous school, health fund details **for parents:** name, physical address, email address, phone number, date of birth, vehicle registration details, occupation, doctor's name and contact information, other children's details, maiden name of ex-pupils, alumni year, whether alumni had further education, professional experience and personal news **for job applicants, staff and contractors:** name, company name and ABN, phone number, physical address, email address, date of birth and age, contact details of next of kin, emergency contact numbers, including doctor, residency status/work visa status, qualifications, education, academic transcript, work permit, details of referees, marital status, record of interview, leave applications, photograph, applications for promotions, references, commencement date, employment agency details, former employers.

Data | Tier 3

Data Definitions	Data Examples
Non-PII data. Data not falling into either the High or Medium sensitivity tiers. Data in this tier is typically in the public domain or presumed to pose low or no risk.	Data assumed to be in public domain or low / no risk data

Functionality / Purpose of service & Reasonableness | Tier 1

Functionality	Reasonableness
Products which offer generic functionality in any of the following categories will be deemed as falling into tier 1: • Remote access Products in the following broad product categories will be deemed as tier 1: • Learning Management / Student management and learning support systems e.g., student work, assessment, academic results, timetabling, pastoral care, communication; • School administration systems, including student records, attendance, data collection e.g., enrollment, consent management; • Financial management / payment collection systems;	Products which may contain, display or promote the following categories of information will be deemed as falling into tier 1: • Advertising of products/services in the following categories: alcohol, controlled or banned substances, gambling, tobacco products, firearms and firearm clubs, adult products and pornography. • Any function or display of information which may be deemed offensive by a reasonable member of the school community (eg racist, sexist content)