Department of Education

Vendor/Supplier - Security and Privacy Risk Assessment

Application / Solution:		**SECCA App**	
Vendor name:	SECCA: Sexuality Education, Counselling & Consulting Agency Inc.		
Description:	A digital web-based resource to help teachers deliver relationships and sexuality education to all students, designed with additional learning needs in mind.		
Report date:	23/09/2022	**Questionnaire submission date:**	2/09/2022
Intended users:	Students, Teachers, Admin and Parents	**Licensing model:**	Freeware
Data sensitivity rating:	Restricted	**Consent to share results: ***	No - do not share
Risk Rating:	**Low**		
Consent Rating:	**Notification**		

*Vendors were asked if they were willing to share the assessment data and results with other educational jurisdictions in Australia

Information Types Stored/Managed by Solution

Staff/teacher name	x	Student email address	x	Student biometric data	
Staff/teacher email address	x	Student date of birth		Student geolocation data	
Staff/teacher personal information		Student work/content	x	Student grades or performance data	
School Name	x	Student attendance records		Student other data	
Staff/teacher other data		Student behavioural records		Parent name	x
Student name	x	Student photos or videos	x	Parent contact information	x
Student home address		Student gender		Parent financial data	
Student telephone number		Student medical or health data		Parent other data	

Risk Area & Recommendations

Area:	**Governance**	**Rating:**	**Amber**

The Supplier maintains some aspects of security governance over the operations of the service provided to DOE, but there are noted gaps against security best practice specifically around published policies, standards and embedded practices and processes.

Questions that contributed to this rating include:

-	COM10	Maintain an ISMS	No Compliance
-	COM11	CISO or CSO	Shared responsibility
-	COM13	Security related policies and standards	Minimal Compliance
-	DSE7	Police background checks (employees/contractors)	Initial onboarding
-	SEC3	Security assessment results available to customers	Not provided

Area:	**Supply Chain Risk Management**	**Rating:**	**Amber**

The Supplier maintains some aspects of security governance over the operations of the service provided to DOE, but there are noted gaps against security best practice specifically around published policies, standards and embedded practices and processes.

Questions that contributed to this rating include:

-	SOL1	Hosting solution architecture	Third party infrastructure
-	SOL7	Usage of third-party software code	open source code/service
-	DSE5	Outsourced solution/database support	Yes - data access

Area:	Access & Authorisation	Rating:	Yellow

System access management is handled by the Supplier in a manner that is mostly compliant with security best practice. In order to be fully compliant and ensure that unauthorised access is controlled, further process and configuration enhancements may be required, including requirements for identification, authentication, and credential/password management.

Questions that contributed to this rating include:

-	SOL3	Physical access to infrastructure and data	Admin staff (external)
-	SOL4	Physical access controls	Physical locks
-	DSE9	Prevention of copying or theft of data	No controls in place
-	ACC4	Account management	Individual
-	ACC6	Role based access	Minimal Compliance
-	ACC7	Multi-factor authentication (MFA) deployed	No support for MFA

Area:	Data Security	Rating:	Green

The supplier demonstrates a sufficient level of compliance within this category area.

Area:	Security Monitoring & Incident Mgmt	Rating:	Amber

Some of the process, practices and systems used to detect and respond to adverse security events and incidents are in place but are below the levels required for effective risk management. Policy and procedural enhancement, as well as the deployment of robust detection systems are required to achieve a satisfactory maturity for incident management.

Questions that contributed to this rating include:

-	LOG1	System logging	Yes - Minimal logging
-	LOG2	Length of system log retention	Maximum 30 days
-	LOG4	Security logging	Yes - Minimal logging
-	LOG5	Length of security log retention	Maximum 30 days
-	SEC1	Vulnerability assessments performed	Manual Testing (annual)
-	SEC2	Penetration testing performed	Manual Testing (annual)

Area:	Privacy	Rating:	Green

The supplier demonstrates a sufficient level of compliance within this category area.

Area:	Solution Maturity	Rating:	Green

The supplier demonstrates a sufficient level of compliance within this category area.

Area:	Legal & Contractual	Rating:	Green

The supplier demonstrates a sufficient level of compliance within this category area.

Vendors may be invited to be re-assessed based on a number of factors, including time since original assessment, updates to the Department of Education WA standards, updates to the vendor product/service and/or occurrence of a breach or security incident.
Vendors must not claim or imply that this report is an endorsement, recommendation, or approval of the product/service or a guarantee that the service is fit for purpose.