SCHEDULE A: PRIVACY BREACH RISK MATRIX

This Schedule is pursuant to the Privacy Breach Management Procedure. Approved by the Vice-Chancellor on 14 December 2020.

	Scope of Data	Currency	Accessible	Regulatory/Contractual Requirements
Extreme	• highly sensitive information with serious risk of physical, reputational, emotional, financial harm, identity theft to large number of people (>100) • breach involves security-classified information at Protected or higher	• information is up to date and can be used to detriment of individual	• information accessible • not encrypted or does not require specialist knowledge to make it useable	• breach of Deakin's contractual data protection obligation to third party • reportable under Mandatory Data Breach (MDB) notification scheme (Privacy Act/General Data Protection Regulation/UK Data Protection Act) • information transferred or stored outside Australia and no or inadequate privacy protection in place.
Major	• risk of physical, reputational, emotional, financial harm, identity theft to large number of people (<100)	• information is up to date and can be used to detriment of individual	• information is accessible • not encrypted or does not require specialist knowledge to make it useable	• breach of Deakin's contractual data protection obligation to third party • reportable under MDB notification scheme) • information transferred or stored outside Australia and no or inadequate privacy protection in place.
Moderate	• risk of reputational or emotional harm/embarrassment, • no risk of physical or financial harm, identity theft • modest number of people involved (<50)	• information is up to date	• information is not encrypted or does not require specialist knowledge to make it useable	• no contractual obligations to third party • no MDB notification requirements
Minor	• no financial or sensitive information involved • no risk of emotional or reputational harm • individual name/email/address revealed in combination with other innocuous information (e.g. course identifier, unit allocation) • < 5 people involved and can be managed within the operational unit	• information is up to date	• information is accessible • information cannot be retrieved before reading	• no contractual obligations • no MDB notification requirements

TABLE 2: LIKELIHOOD RATINGS TABLE

Likelihood of events or consequences is determined by asking- has it happened before? If so, how often (taking consideration of time-related factors and volatility)? What is known or reasonably ought to be known about the risk. There may be data to assist. We can further gain an estimate of likelihood by not only asking the question in relation to Deakin – but also the sector or similar institutions (dependent on effectiveness of existing controls).

Likelihood Rating	Description
Almost Certain	• Almost certain to occur/happen or is imminent, possibly frequently in a year. There is a history of regular occurrence at Deakin.
Likely	• Will probably occur/happen, but not a persistent issue. There is a history in the recent past (within 3 years) of occurrence at Deakin.
Possible	• Likely to happen occasionally and has a reasonable chance of occurring at Deakin.
Unlikely	• Not expected to happen, but it is a possibility in the sector.
Very Unlikely/ Rare	• Very unlikely this will happen.

TABLE 3: RISK MATRIX TABLE

		Consequence				
		Extreme	**Major**	**Moderate**	**Minor**	**Insignificant**
Likelihood	**Almost Certain**	**Very High**	**Very High**	**High**	**High**	**Medium**
	Likely	**Very High**	**High**	**High**	**Medium**	**Medium**
	Possible	**High**	**High**	**Medium**	**Low**	**Low**
	Unlikely	**High**	**Medium**	**Low**	**Low**	**Low**
	Very Unlikely/ Rare	**Medium**	**Medium**	**Low**	**Low**	**Low**

TABLE 4: CONTROL RATINGS TABLE

How effective are the current controls in relation to reducing the likelihood or consequence of the risk?

Not Effective	**Significant control gaps (controls associated with the risk are extremely weak and/or non-existent) that result in the control not influencing the risk level.**
Mostly/ Partially Effective	**Some controls are established however improvements/ further developments are required to remediate control gaps/ or there are factors outside of our control. The control is influencing the risk level, however actions are needed to strengthen processes and documentation or further understanding is required of external factors.**
Effective	**Controls are established and effective in mitigating risk; with no controls gaps. The control is influencing the risk level and there is evidence of adequate processes and documentation. Only monitoring is needed. The strength of this control environment means that if this risk eventuates, it is most likely as a result of external circumstances outside of Deakin's controls.**

TABLE 5: RISK RATING - MANAGEMENT/MITIGATION ACTION REQUIRED

Risk Rating	Mitigating Action Requirements
Very High	**University Executive management responsibility. Cease or isolate source of risk. Immediate attention, response and treatment required prior to commencement or continuation of work. Requires a risk assessment and risk management plan by the relevant Executive for approval (prior to work commencing or continuing) by the Vice-Chancellor, Risk oversight by Council, Audit and Risk Committee (ARC) or nominated Standing Committee.** The Risk must be escalated to the responsible University Executive member(s) immediately for full consideration and approval of risk mitigation/ opportunity measures with the Vice-Chancellor.
High	**Faculty General Manager/Director/Head of School management responsibility. Implementation of risk controls to be given appropriate attention, response and demonstrably managed. Executive approved risk treatment required prior to commencement or continuation of work.** Risk must be escalated to the responsible Director, Faculty General Manager or Program/ Project Manager immediately. Vice-Chancellor informed by the appropriate University Executive for consideration of risk mitigation measures to lower risk level.
Medium	**Faculty General Manager/Director/Head of School responsibility. Assess the risk, determine whether current controls are reasonably practicable for the task/ work area/ environment or if further action/ treatment is required. All risk mitigation factors to be explored and exhausted before proceeding. Monitor, review and document controls through regular business practices or local area meetings.** Risk must be escalated to the responsible Director, Faculty General Manager or Program/ Project Manager for consideration.
Low	**Local Management responsibility Faculty/Portfolio/Project management responsibility. Managed by routine procedures, monitor and review as required.** Managed within Faculty, Portfolio or Project by well-established routine processes/procedures with established controls.