Schedule 1 – Security Classification Levels

Classification	Definition	Operational Impact if compromised	Examples
Restricted	Information that is highly sensitive and intended to be used by a small, limited number of authorised individuals on a need-to-know basis.	Unauthorised disclosure may result in extreme or severe impact to RMIT such as: • Severe financial harm • Significant harmful reputational damage • Extreme regulatory penalties or loss of key licenses and/or funding • Significant interruption of critical operational system/processes • Significant impact to research activity • Severe risks to the safety or wellbeing of individuals	Security vulnerabilities, confidential out-of-court settlements, records affecting national security, protected disclosures, unpublished cybersecurity research, Records including the following government issued unique identifiers that identify individuals: driver's license number, national identification number, Centrelink account number, Tax file number, Medicare account, Passport number.
Protected	Information that is personal and/or sensitive and intended to be used by authorised individuals for an authorised purpose on a need-to-know basis	Unauthorised disclosure may result in severe or major impact to RMIT such as: • Major financial harm • Major harmful reputational damage • Major regulatory penalties or loss of key licenses and/or funding • Major interruption of critical operational system/processes • Major impact to research activity • Major risks to the safety or wellbeing of individuals	Information relating to ongoing commercial or research projects where disclosure could jeopardise the project, personal identifiable information, unreleased student results, banking details, information related to discipline, grievances, salary information, audit reports, strategic and governance documentation, medical and health information
Trusted (default)	Information that is intended to be used internally in the day-to-day operations of RMIT	Unauthorised disclosure may result in moderate or minor impact to RMIT such as: • Minor financial harm • Minor harmful reputational damage • Minor regulatory penalties or loss of key licenses and/or funding • Minor interruption of critical operational system/processes	User manuals, training manuals and documentation, employee newsletters, meeting minutes, de-identified clinical research

Classification	Definition	Operational Impact if compromised	Examples
		• Minor impact to research activity • Minor risks to the safety or wellbeing of individuals	
Public	Information which has been authorised by the trustee for public access and circulation	Unauthorised disclosure causes minor or negligible impact to RMIT	Information authorised to be available on or through RMIT's website, publicly available campus brochure, publicly available campus map, published annual report, information in the public domain, job postings