Acceptable Use Standard – Information Technology

What is it?

This standard is a resource to the RMIT Information Technology and Security Policy.

It outlines the required behaviours for all users of RMIT information technology (IT) assets and services. The aim is to ensure all access and use of RMIT information systems and IT services is appropriate, legal, safe and fair for all users while ensuring the protection of RMIT Systems and Data.

The standard describes typical IT- related activities that are considered acceptable and unacceptable. It includes management data, emails, connecting to and using the internet, the RMIT network and software as a service. Unacceptable behaviours are those that are illegal, in breach of any RMIT policy, harms others, harms the University or prohibits fair use of IT services by other users.

Who is this for?

This standard applies to all individuals who are required to comply with the RMIT Information Technology and Security Policy.

Contents

1. RMIT requirements

1.1. Acceptable use of University IT

Standard	Description	Examples
AU-010	Access and use of IT systems and facilities must be for legitimate university purposes, specific to your role	Learning, teaching, research, and University operations activities
AU-020	Access and use of IT facilities for reasonable personal or recreational purposes is acceptable, provided; such use does not adversely affect other IT users such use is legal Use of IT facilities is a privilege, not a right, therefore may be withdrawn at any time at the discretion of the Chief Information Officer (CIO) or the Chief Information Security Officer (CISO)	Booking a movie ticket Checking your child's school website Filling University storage with personal data, videos etc would be unreasonable
AU-030	As part of employment, staff must complete Cybersecurity and IT related training modules when requested	

1.2. Unacceptable use of University IT

Standard	Description	Examples
AU-040	Creating, using, saving, accessing or distributing material that might reasonably be considered offensive, obscene or indecent by an ordinary member of the public, or is illegal	pornographic, racist or sexist material
AU-050	Plagiarising, copying or distributing information in contravention of copyright or similar legal obligations without the owners' express permission	copyright images, text messages, videos, memes or sounds from websites owned by a third party
AU-070	Using IT systems to harass, bully, defame	Spreading of malicious information via email
AU-080	Unauthorised attempts to interfere with the operation of, or make University IT systems or services unavailable	Flooding a booking system with fake bookings
AU-090	Sharing or disclosure of personal user identities, passwords, or security codes. Passwords must not be written down or left in a place where an unauthorised person might see them	Giving your password to someone to log in to check your email or book meetings from your account
AU-100	Unauthorised hacking or probing for security vulnerabilities in networks, systems or university applications etc. without the written consent by the Chief Information Security Officer	Students or staff probing Canvas for vulnerabilities to exploit
AU-110	Creating, introducing or distributing computer viruses or other malicious software onto any University network device or system	Knowingly sending email with attachments containing a virus to any other user.

Standard	Description	Examples
AU-120	Disclosing, removing or disposing of information assets including both physical and information assets without authority from ITS, College or portfolio executive management. Such authority must comply with all University policies, including the Information Governance policy	Taking a monitor home or using a staff contact database without permission Destruction of RMIT records within the mandated legal period
AU-130	Connecting any IT devices or systems to the University network deemed by the CISO to be insecure.	Connection of a computer that is not patched with current software and operating system Refer to cybersecurity website for guides on how to configure security settings on your personal devices
AU-140	Monitoring, intercepting or accessing network traffic, emails, files etc. intended for another person	Access to another staff's email account
AU-150	Using University IT facilities to conduct non-University related business, whether for profit or other purpose	Using RMIT technology to run a business or charity unrelated to the University, including setting up crypto coin mining
AU-160	Excessive use of IT storage or processing capacity such that other users are negatively impacted	A staff member or student storing excessive data, (either personal or University related) on University storage systems
AU-170	Deliberate unauthorised access to systems or data and/or Unauthorised use of data or information obtained from Information Systems	Using someone's unlocked computer to act on their behalf
AU-180	Storing non-public information on non-RMIT endorsed site or location such as a USB drive, cloud storage or forwarding RMIT email with attachments to your personal email account	Saving a student class listing on a personal storage service such as personal Dropbox or Box etc. Cloudstor and Office 365 are endorsed locations
AU-190	Entering into contractual relationships or making other legally binding commitments on behalf of the University without the appropriate governance, approvals, contractual reviews and vendor engagement	Signing up to a software service in the name of RMIT
AU-200	Representing the University or its entities without the explicit authorisation of College, portfolio executive management or Council to do so	Posting on social media or signing a software agreement as an RMIT representative

Standard	Description	Examples
AU-210	Disclosing non-public information through websites, blogs, discussion forums etc.	Do not send a Facebook post saying where your manager lives.
AU-220	Transmission of unsolicited commercial advertising material or any other form of unsolicited commercial electronic message, including material commonly known as “spam”, or “junk email”	Perpetuating chain letters, virus warnings or hoax messages (don’t send spam!)
AU-230	Responding to spam or phishing messages by supplying non-public RMIT or personal information	Don’t deliberately respond to spam or phishing messages
AU-240	Using commercial VPN services to access Geo-Locked content while on the RMIT network or to use RMIT services is not permitted	E.g. MobileVPN, ExpressVPN etc.
AU-250	Using applications on RMIT computers that allow for remote control of those computers from other locations	E.g. TeamViewer, AnyDesk etc.

1.3. Email usage

Standard	Description	Examples
AU-300	RMIT supplied Outlook is the only E-Mail software approved for use by the University. All users must only use their RMIT issued email account within O365 email system. No other E-Mail software is permitted.	Google Mail is no longer approved for use. Apple Mail, Thunderbird or other email software are NOT to be used
AU-310	RMIT may block any email, inbound or outbound, that threatens the security of University systems and data, involves the dissemination of spam, or includes content that is against any University policy	
AU-320	Anyone with an RMIT email address must not set up auto forwarding of RMIT email to non-RMIT provided devices or personal email accounts	Setting up forwarding to your personal email account so you can view or work on RMIT emails at home is not permitted
AU-330	All emails remain the property of RMIT and may be monitored, retained or deleted in line with all RMIT policies	When you leave RMIT your emails remain the property of the University and may be retained as legal University records
AU-340	Former staff returning to RMIT employment may get access to their past emails if they return to their former role (or by policy exemption approved by RMIT CISO).	A casual lecturer returning to the same role after a year off

Standard	Description	Examples
AU-350	Emails must be classified using the RMIT information classifications be based on the sensitivity of information contained in the email, including any links and attachments. All Office 365 documents including email and O365 attachments must be labelled with the appropriate classification wherever the classification labels are available to the user	An email containing an attached payroll report must be labelled 'protected' or Restricted' using Outlooks sensitivity labels
AU-360	Use of shared (group) email boxes must be configured such that the person sending the email is identifiable to the recipient. At least two people should share ownership of the mailbox. Email to groups of recipients must be for legitimate university purposes, specific to your role	
AU-370	Non-public information must not be shared with recipients who do not need that information for a legitimate University purpose. (See also the RMIT Privacy Statement on appropriate use and disclosure of personal information.)	

1.4. Software and application security

Standard	Description	Examples
AU-400	Downloading, installing or running software, applications or software as a service (SaaS) that are not endorsed by ITS is prohibited	Bitcoin miner, SpeedUpMyPC etc. Lodge a request with ITS if you need to install additional software
AU-410	RMIT software procured by or licensed to, the University should not be copied or re-used by un-licenced users. This includes computer software and cloud services	Adobe Photoshop, VMWare Player etc
AU-420	All software developed within RMIT is the property of RMIT and must not be copied or distributed without prior written authorisation	Research software, custom code for applications
AU-430	Users are not permitted to tamper with or disable any installed security software (e.g. anti-virus software). Installed security software must be kept running at all times	Changing settings for Antivirus or System Configurations

1.5. Physical security

Standard	Description	Examples
AU-500	All workstations must be screen locked if the workstation is left unattended.	Toilet break, meeting, kitchen visit
AU-510	Hardware or software must not be taken offsite without prior authorisation from ITS or relevant Portfolio manager	Taking a computer monitor home for remote working
AU-530	All workstations including laptops must be physically locked to the desk when not in use for extended periods.	This includes overnight or for extended periods in worktime (more than an hour).

Standard	Description	Examples
AU-540	Materials containing non-public information must not be left unattended.	PowerPoint printouts or marked whiteboards or flip charts left in a meeting room or by a printer

1.6. Employee behaviour

Standard	Description	Examples
AU-610	Protect RMIT Information everywhere • ensure you are not overheard when discussing RMIT related matters in public • ensure all non-public printed or digital information is kept discrete and secure in a public space • when taking photos or videos in RMIT office environments do not allow student or staff personal information to be included within the photo or video and do not shared on any social media forum	Be aware of being overheard when discussing confidential RMIT information such as a work call on your way home on the train
AU-620	Access, use and share only on a need to know basis • ensure you are authorised to share protected or restricted information and ensure the recipient is authorised to receive it • share only the minimum information required for the task	
AU-630	Disposal of physical information and assets • use secure waste when disposing of non-public hard copy information • return all RMIT equipment due for disposal ITS	

AU-640	Play your role in keeping RMIT safe
	• if you suspect your password is compromised, you must change it immediately and report it to the ITS service and support centre
	• passwords must not be written down or left in a place where an unauthorised person might discover them.
	• your RMIT password must not be used for non-RMIT applications or services
	• any event that may put RMIT information or systems at risk of compromise or unauthorised disclosure, whether accidental or intentional, must be reported to:
	  ○ your line manager; and
	  ○ ITS Service and Support Centre
	• Staff must immediately forward email they suspect are malicious to reportphishing@rmit.edu.au or call the ITS Service and Support Centre	

1.7. Monitoring

Standard	Description	Examples
AU-700	RMIT conducts surveillance across all systems and devices to determine any security weakness or policy non-compliance	
AU-710	RMIT may confiscate any RMIT device assigned to an individual in order to complete security or forensic investigation	
AU-720	RMIT may remotely lock, wipe or reconfigure any University issued device if it is deemed to be a security risk	

2. Information security standards exemptions

2.1. Exemptions from the Information Technology and Security Policy and related standards must be sought using the ITS policy exemption process determined by the Chief Information Security Officer.

3. Compliance

3.1. Repeated non-compliance with this standard may result in University disciplinary action, or legal action in cases of illegal activity. Management will decide what action to take, if any, based on the severity of the incident(s).

3.2. All staff are collectively and individually accountable for minimising information security risks, ensuring data privacy and avoiding information security incidents.

More information

These are not exhaustive lists. Speak to your manager, HR, the ITS Service and Support Centre or the if you are uncertain whether other activities are acceptable or not, or you are uncertain about whether a standard applies to a given situation.

Please refer to the below for further information:

- Information security data protection sensitivity labelling – assigning appropriate data labels
- RMIT cybersecurity webpage – cyber advice and FAQs
- Information Governance Policy
- Privacy Policy

Document history

Version	Effective date	Authority	Author	Register reference
1.1	5 May 2020	Information Technology and Security Policy	Chief Information Officer	POL/2020/00009[V2]