Monash University Procedure

Procedure Title	Electronic Information Security – Minimum Security Controls Procedure
Parent Policy	Electronic Information Security Policy
Date Effective	01 August 2017
Review Date	01 August 2020
Procedure Owner	Chief Information Officer
Category	Operational – Information Technology
Version Number	1.0
Content Enquiries	IT Service Desk - http://monash.edu/esolutions/contact Security@monash.edu
Scope	• All campuses in Australia • Monash South Africa • Monash College Pty Ltd • Monash Malaysia. • All staff, students and other Authorised Users
Purpose	Define the controls required for the information according to their classification
PROCEDURE STATEMENT	

1. General Requirements

Systems according to their classification must comply with the controls shown in the following tables

Monash University Procedure

Required Controls based on Information Asset's Confidentiality classification.

Controls		Confidentiality - Classification			
		Critical (4)	**Protected (3)**	**Restricted (2)**	**General (1)**
Authentication	Single Sign-On	Required			Optional
	Authentication Method	Multifactor	Multifactor (Risk Based)[2]	Standard	Optional
	Password ageing			Yes	Optional
	Automated Password Strength Checks			Yes	Optional
	Password Reuse			Max Value	Optional
	Login attempts before lockout	5 unsuccessful attempts		10 unsuccessful attempts	
	Account Unlock	Manual	Manual of self service system	Manual of self service system	Optional
Penetration Tests		Required		Optional	
Remote Access	Monash Staff	Least Privilege (Risk Based)[3]		Least Privilege	Optional
	Vendor Staff	Least Privilege (Risk Based)[3]		Least Privilege	Optional
Web Application Firewall	Web applications only	Required		Optional	
Malware Protection		Required			
Access Control	Role Based	Least Privilege			Optional
	Rights Review	Semi Annual		Annual	Optional
Security Monitoring	Event Logging	Access, modification	Access, modification	Access	Access
	Reporting	Real Time		Weekly	Monthly
	Retention of Logs	90 Days	60 Days	30 Days	Optional
Session Timeout		10 Minutes		15 Minutes	30 Minutes
Encryption	Email	Required		Optional	
	Transmission	Required			
	Storage	Required		Optional	
	External Media(Discs, USB Drives, External Drives, Third party cloud storage services not provided by Monash)	Required		Optional	
	Data Backup	Required		Optional	
Version Control		Required		Optional	
Information Disposal[1]	Cloud Servers	Purge		Clear	Optional
	External Media	Destroy		Clear	Optional
	Monash Data Centre Servers	Purge			Optional

1. Subject to data retention and archiving policies and procedures.
2. Standard could be used as result of the risk assessment.
3. Access could be denied as result of the risk assessment.

Monash University Procedure

Required Controls based on Information Asset's Integrity classification.

Controls		Integrity - Classification			
		Absolute (4)	**High (3)**	**Moderate (2)**	**Low (1)**
Authentication	Single Sign-On	Required			Optional
	Authentication Method	Multifactor	Multifactor (Risk Based)[2]	Standard	Optional
	Password ageing			Yes	Optional
	Automated Password Strength Checks			Yes	Optional
	Password Reuse			Max Value	Optional
	Login attempts before lockout	5 unsuccessful attempts		10 unsuccessful attempts	
	Account Unlock	Manual	Manual of self service system	Manual of self service system	Optional
Penetration Tests		Required		Optional	
Remote Access	Monash Staff	Least Privilege (Risk Based)[3]		Least Privilege	Optional
	Vendor Staff	Least Privilege (Risk Based)[3]		Least Privilege	Optional
Web Application Firewall	Web applications only	Required		Optional	
Malware Protection		Required			
Access Control	Role Based	Least Privilege			Optional
	Rights Review	Semi Annual		Annual	Optional
Security Monitoring	Event Logging	Access, modification	Access, modification	Access	Access
	Reporting	Real Time		Weekly	Monthly
	Retention of Logs	90 Days	60 Days	30 Days	Optional
Session Timeout		10 Minutes		15 Minutes	30 Minutes
Encryption	Email	Required		Optional	
	Transmission	Required			
	Storage	Required		Optional	
	External Media(Discs, USB Drives, External Drives, Third party cloud storage services not provided by Monash)	Required		Optional	
	Data Backup	Required		Optional	
Version Control		Required		Optional	
Information Disposal[1]	Cloud Servers	Purge		Clear	Optional
	External Media	Destroy		Clear	Optional
	Monash Data Centre Servers	Purge			Optional

1. Subject to data retention and archiving policies and procedures.
2. Standard could be used as result of the risk assessment.
3. Access could be denied as result of the risk assessment.

Monash University Procedure

Required Controls based on Information Asset's Availability classification.

Controls		Availability - Classification			
		Mission Critical - A (4)	**Business Essential - B (3)**	**Business Supporting - C (2)**	**Low Availability - C (1)**
Disaster Recovery	Documented Plan	Required		Optional	
	Plan's Annual Test	Required		Optional	
	Data Backups	Required		Optional	
	High Availability Architecture	Required		Optional	

Monash University Procedure

Responsibility for implementation	Chief Information Officer Information Owners Deputy Vice-Chancellors Vice Presidents Pro Vice-Chancellors and President, Monash South Africa Deans of Faculties
Status	New
Approval Body	**Name:** Chief Information Officer **Meeting:** N/A **Date:** 01 – August - 2017 **Agenda item:** N/A **Author:** Cesar Guzman – IT Security and Risk Consultant.
Definitions	**Least privilege:** requires that in a particular abstraction layer of a computing environment, every module (such as a process, a user, or a program, depending on the subject) must be able to access only the information and resources that are necessary for its legitimate purpose **Self-service system:** Self-service software allows people to secure answers to their inquiries and/or needs through an automated interview fashion instead of traditional search approaches **Version Control:** is a system that records changes to a file or set of files over time so that you can recall specific versions later. **Purge:** applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques **Destroy:** renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data **Clear:** applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).
Legislation Mandating Compliance	As per parent policy
Related Policies	As per parent policy
Related Documents	IT Security and Risk Framework IT Risk Management Manual Risk Management Procedures