Information Technology Principles and Standards
University of Otago

Gareth Wood, IT Enterprise Architect

Document Version: 2.0, Tuesday 19 September 2023

University Operations

Information Technology Services

Campus and Collegiate Life Services | Campus Development | Chief Operating Officer
Health and Safety Compliance | Project Management | Property Services
Risk, Assurance and Compliance | Shared Services | Sustainability

University of Otago | PO Box 56 | Dunedin 9054 | New Zealand

Enable | Engage | Experience

Document Version Control

Version No.	Date	Revision Details	Author	Endorsed	Approved
0.9	29 May 2018	Incorporating feedback from all earlier drafts. Correcting formatting and grammar.	David Maclaurin	-	-
0.92	10 June 2018	Executive Summary and final edits.	David Maclaurin		
0.95	25 June 2018	Added standard governing use of AI, Machine Learning, Deep Learning systems. Added standard for use of enterprise service bus	David Maclaurin		
0.98	29 June 2018	Table formatting	David Maclaurin		
0.10	28 November 2018	Insert IT Governance Landscape image and check content	David Maclaurin		
0.11	28 Feb 2019	Insert Cyber Security Principles and refer to CSFPrinciplesV001 document. Final updates.	Dave Maclaurin & Richard Feist		
0.12	5 Mar 2019	Final feedback incorporated	Dave Maclaurin		
1.0	8 April 2019	Additional edits and reset version number for 1.0 first official release	Dave Maclaurin	By IT Governance Board 28/3/19	By IT Governance Board 28/3/19
1.1	16 February 2022	Added Information Management principle	Jack Heikell		
2.0	21 February 2023		Gareth Wood Sherif Samy		
Document ID:		OUR Drive URL			

Contents

Executive Summary

Enterprise architecture focusses on optimising peoples' interactions with information technology to ensure that IT investment and effort best supports the strategic objectives of an organisation over time.

This document presents a set of IT principles and standards, primarily to help guide University Professional staff engaged with information technology, in their support of the strategic objectives and policies of the University of Otago, and of its staff and students.

The contents of this document align with Information Technology Services strategies and roadmaps.

The IT principles set out here inform themes and approaches to Information Technology at the University of Otago. Each principle is broadly applicable to a range of IT roles and activities.

The IT standards apply across a selection of IT subject domains. Their objective is to consolidate and simplify the approach to specified aspects of IT, and to provide guidance that will help address identified IT domain problems.

While this document is primarily intended for an audience of Professional staff engaged with IT, parts of it may be of value to all University Staff.

A glossary of terms is provided at the end of this document.

Introduction

The following principles and standards are provided to inform and direct IT related activities, including the creation of service specifications, project and procurement activities, IT governance tasks, and IT related BAU and implementation tasks for University of Otago IT services.

The IT principles and standards are not intended to be a 'one solution fits all' reference manual, rather they comprise a set of statements that present best practices and approaches that will improve the way we use IT at the University.

The contents of this document support existing and proposed IT strategies and roadmaps and incorporate a number of elements of IT best practice. This document also supports the University of Otago 3PM methodology for robust project lifecycle management.

Suggestions for further improvements to this document are welcome at any time.

This document will be reviewed at yearly intervals from the initial date of publication. An updated version will be republished with highlighted changes when required.

Audience

The primary audience is Professional staff that provide or support IT services for the University. The secondary audience is other Professional staff and Academic staff.

How to use this document

- Staff must take all reasonable steps to support and abide by the principles and standards in this document.
- Academic freedom in research and teaching is understood and supported. If these freedoms are exercised with respect to the design or use of IT technologies, please ensure that other University IT services, systems and processes are not adversely impacted, and that cyber security controls are not compromised. If you are unsure, please contact the ITS Director or Enterprise Architect to discuss your situation before proceeding – we are here to help.
- If circumstances arise that may preclude support for any of these IT principles or standards, please obtain approval from the ITS Director or Enterprise Architect prior to proceeding.

Reference Documents

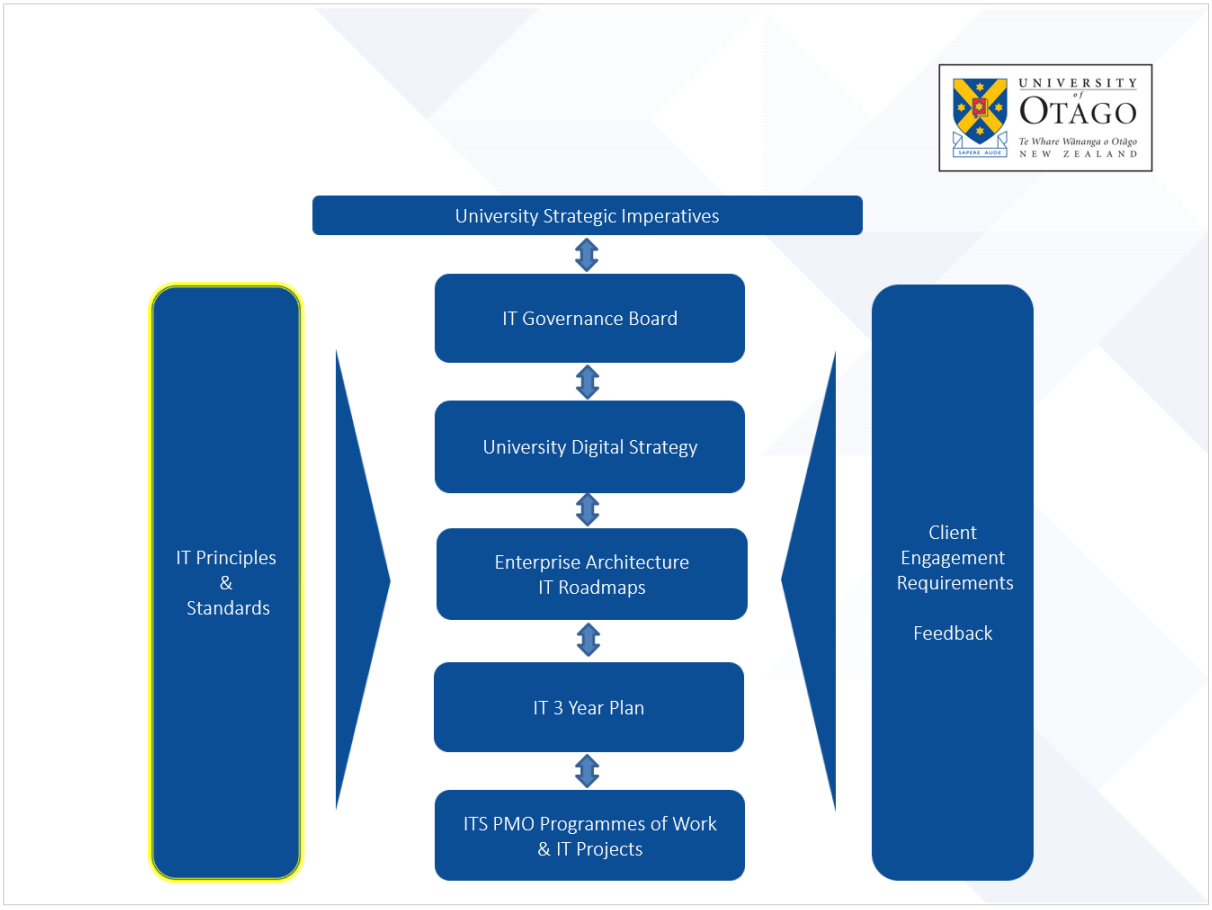
1. *Register of Preferred University of Otago Services and Solutions*
2. *Register of University of Otago Primary Data Sources*
3. *Register of University of Otago Cloud Providers*
4. *Register of Existing University of Otago IT Systems and Services*
5. University of Otago Cloud Risk Assessment Tool
6. AI Adoption Principles for Tertiary Education. Research Centre of Artificial Intelligence and Public Policy, University of Otago
7. *University of Otago Cyber Security Framework, Policies, Procedures & Standards*
8. *OurDrive 3PM site: https://ourdrive.otago.ac.nz/ou-projects/Pages/ProjectDocumentTemplates.aspx*

Note: Feb 2019, italicised documents in this list are in-process and will be published at a later date. Please contact the IT Enterprise Architect if you require early access to any of these.

Supporting IT Governance at Otago

The diagram below illustrates major activities and collateral supporting the IT Governance function at Otago.

The IT **Principles and Standards** document is highlighted in yellow, and the arrow beside this component illustrates its relationship to the overall IT Governance function.



Enterprise Architecture Overarching Principles

Enterprise Architecture Principles

General

EA PRINCIPLE: General	RATIONALE
➢ Keep IT simple	IT services must be as simple, reliable and sustainable as possible while meeting the needs of the organisation. Minimise complexity wherever possible.
➢ IT is about supporting people	Aim for the most effective and efficient IT services footprint that delivers the most practical value to the greatest number of people at the lowest cost.
➢ IT Services distil and reflect the positive values of our University and its people	Use of information technology reflects University of Otago values and plays to our strengths. It is inclusive, innovative, collaborative, easily understood, has a clear purpose and helps us all succeed.
➢ Focus on the delivery of high value services directly to our clients	Over time refocus our IT services and expertise to deliver more direct value to our clients.
➢ Geographic isolation or distance is not a barrier to research or other academic collaborative initiatives	We strive to ensure that IT services can be 'globally enabled' as required. They use appropriate, approved delivery and integration technologies to ensure that our academic staff and students can seamlessly collaborate around the world.
➢ Deliver the fewest IT services to meet requirements, ensure each is aligned to University strategies, and deploy them widely	We do not duplicate IT services or unofficially repurpose existing IT services. We support the implementation of a single enterprise wide IT architecture and set of design patterns that are themselves aligned to the strategic goals of the organisation.
➢ Sustainably reuse existing IT infrastructure and services	Where practicable we sustainably reuse our network, infrastructure, identity, data, software and other IT services; we only procure or build new (on-premises or cloud) IT services when no suitable existing solution exists.
➢ Sustainability becomes a part of our IT decision making and operational perspective	When procuring infrastructure, we favour solutions with demonstrably less environmental impact. We configure our devices and IT services to minimise energy use. We design and run our data centres to minimise environmental impacts, and we favour cloud providers that take practical steps to minimise their environmental impact.

EA PRINCIPLE: General	RATIONALE
➢ Always consider cloud services when planning any new IT solutions	Cloud services provide new IT delivery options and toolsets that can be of great value when used appropriately. They also free up our technical staff to work on higher value projects that are of more direct relevance to our clients. Choose SaaS before PaaS before IaaS cloud services. For IaaS and PaaS services, prefer those that support a seamless hybrid cloud deployment model. A *Register of University of Otago Cloud Providers* will be made available. This will list existing approved providers that the University has already selected and contracted with and will include details on the services being provided. A *University of Otago Cloud Risk Assessment Tool* will be made available to help guide project teams when selecting a new cloud services provider.
➢ New IT services share default capabilities	New IT services are designed and implemented to be highly available where possible; easily maintained and patched; able to recover from partial failures and degrade gracefully; are stateless where possible; and able to scale out with minimal effort. Their performance can be measured, logged and easily tuned.
➢ IT services are proactively managed University wide, they are always in a known state. They are stable, recoverable and available	IT services must be: monitored, backed up, patched, included in a disaster recovery plan, highly available and modified via change control processes. Fix any IT service that has recurring issues.
➢ Information Technology Services and Shared Services team roles are adhered to.	Information Technology Services and Shared Services Divisions comprise a number of specialist teams providing specific services, that when combined and orchestrated, deliver IT services to the University. As such it's important that each team focusses on its specific role and set of responsibilities in the organisation, and that each becomes a centre of excellence. Team members do not design, specify, roadmap, deliver or support IT services outside their team's remit or area of expertise.
➢ IT services are developed in accordance with Enterprise Architecture Strategies and Roadmaps	All new IT services, or major modifications to existing IT services, or proposals that might impact on any IT strategies and roadmaps are documented, discussed with, and approved by the IT Enterprise Architect well before any service or financial commitments are made (either internal or external). This ensures that we develop our future IT services and expend funds in accordance with our IT Architecture Strategies and Roadmaps.
➢ IT services support information management requirements by design	All new IT services, or major modifications to existing IT services must consider and support the requirement of Information Management within their design.

Cyber Security

(For additional information regarding the following principles please see: University of Otago Cyber Security Framework Principles)

EA PRINCIPLE: Cyber Security	RATIONALE
➢ Include Cyber Security requirements for new IT solutions	Legislative, regulatory and compliance requirements; both functional and non-functional requirements; identification of information assets and any risks to those assets.
➢ Design secure IT services	IT services are designed and implemented with appropriate security controls in place and these are testable. Consider the type and sensitivity of data held by a service, and the reputational and legal risks if controls fail. IT service security designs anticipate malicious threats and unexpected situations. Security is appropriate to the platforms the service runs on, the user groups for which it is designed, and the locations where it will run. Security designs should not compromise IT service ease of use or functionality.
➢ Identify and manage cyber security risks	Risk mitigations should be effective but must not unnecessarily constrain functionality. Trade-offs between reducing risk and increasing cost should be identified and documented.
➢ Control IT account privileges	IT accounts should only have sufficient privileges for the tasks at hand.
➢ Maintain IT services ease-of-use and manageability when improving security	Security measures should be largely transparent to end users. Administration and configuration of security technologies should not be overly complex or obscure.
➢ IT security defences should be multi-layered and diverse	Greater security is obtained by layering diverse defences around IT systems and services.
➢ Monitor and control the boundaries between compute and storage environments and the networks that connect them	Design common boundaries between compute storage and networking systems to make it easy to monitor and control activity day-to-day and during cyber-attacks.
➢ Identify, strengthen and defend any 'ICT weak links' from cyber attack	It is a fundamental tenet of security that a chain is only as strong as its weakest link. During cyber-attacks a single weak point can be used as a bridgehead, to gain greater and more damaging access to systems.
➢ Segregate IT service components at the network layer if they do not need to interact	Segregating IT components can improve security by ensuring that they cannot be used to gain unrestricted access or control to other unrelated IT services.

EA PRINCIPLE: Cyber Security	RATIONALE
➢ Build or procure IT services that handle failure scenarios safely	Services should always 'fail safe'; i.e. they should protect surrounding IT services, environments, identity and account information and all data.
➢ Keep IT services simple	Complexity is the enemy of IT security. IT systems should be as simple as possible.
➢ Cyber security is everyone's business	All University staff, students and contractors have a role to play if we are to improve IT security. Sharing our experiences and knowledge is key.
➢ Build or procure resilient IT services	Design, procure and operate IT services to limit security vulnerability and to be resilient in response to cyber-attack. IT services must be recoverable in the event of a disaster.
➢ Keep it confidential	All parts of the University computing environment must provide for information integrity and confidentiality.
➢ Support University cyber security policies and procedures	Implement processes, procedures, and systems that comply with organisational security policies.
➢ Accountability Principle	Accountabilities and responsibilities for information systems and services security should be clearly documented.
➢ Awareness Principle	Owners, providers, and users of information systems, must be aware of, and understand, all applicable cyber security policies, responsibilities, practices, procedures.

Enterprise Architecture Standards

Networking

EA STANDARDS: NETWORKING	RATIONALE
➢ There is a single University network provided and managed by ITS	ITS are the sole authorised, wired and wireless network provider for the University. Any proposal, project or plan that will require changes to any part of the University of Otago Network or its ancillary services, or that is likely to alter the performance of the network, must have those changes pre-authorised; this includes any change to access layer cabinets in University buildings. No separate or third-party networks are permitted on any University campus without prior approval.
➢ The new University network is used for new IT services and user devices	Make use of the performance, security and robustness of the new network. New IT services and users' devices must be connected to the new network where possible.
➢ User devices login to the network with University credentials where possible	As the new network is identity based and uses the University's Identity Management System behind the scenes, University usernames & passwords are the best authentication mechanism to use when joining a device to the network.
➢ Devices only connect to a single network at a time	Best practice is to connect to a single network from a single device. A user device connected to more than one network concurrently, by using both wired and wireless connections for example, may experience connectivity issues or data loss.
➢ Protect the University network from external threats	Care must be taken not to join or bridge the University network to any other network unless this is approved and implemented by Information Technology Services. If you need to connect to the University network when off campus, always use the University VPN service and ensure that the device you connect from is patched and secure.
➢ Communicate any proposed building specific networking changes to maintain network performance for all	To ensure good network performance for everyone over time, it is important that the network infrastructure in each University building remains sized and configured appropriately. If you have new specific network performance or equipment requirements, or you are changing a building layout, or the locations where users will connect to the network, you must contact Information Technology Services before any changes or commitments are made.
➢ Multi-user and high throughput IT services are run from the ITS data centres where possible	Multi-user and high throughput IT services are run where possible from the data centres, as these are designed to provide the scalability, security, availability, management and disaster recovery capabilities needed. Having University servers in the data centres, also means that IT services can easily be migrated to run across other cloud platforms in future if required.
➢ Clear identification of users and devices on the network	As we run an identity-based network, all user and headless devices (e.g. printers) connecting to the new network, must be clearly and correctly identified in both the University Identity Management System and Network Registration Portal application as required.

EA STANDARDS: NETWORKING	RATIONALE
➢ Before connecting new types of devices to the network for the first time, consult with Information Technology Services	New types of user devices and research infrastructure, may require specific network changes to best accommodate them.

User Experience

EA STANDARDS: USER EXPERIENCE	RATIONALE
➢ Provide an intuitive, consistent, accessible and simple user interface	IT applications are 'tools' that help people work and study. Their user interfaces must be intuitive and inspire confidence.
➢ Ensure a great desktop and mobile experience	IT applications must perform well and function appropriately for the platform(s) they run on. Users running on different operating systems should have a similar service experience.
➢ Always consider mobile applications	University staff increasingly use a range of compute devices and the use of mobile technologies is increasing. Our approach to application development, user interface design and workflow supports and exploits this trend.
➢ Provide in-application help, built-in troubleshooting capabilities and ensure ease of support	Users must be able to find and use help facilities easily. Support teams must be able to support applications quickly and easily. Prefer applications that provide good self-service help facilities.
➢ Aim for simplicity	A simple application user interface that is easy to use and stable, is preferred over a complex interface that is more challenging to use.
➢ Support internationalisation and accessibility	Applications must support their user base, regardless of their preferred languages. Applications must function well for all users including those with specific accessibility requirements.
➢ Applications must be network and location agnostic	Applications must be able to securely accommodate users who are off campus, or on non-university networks with poor connectivity, as required.

Applications

EA STANDARDS: APPLICATIONS	RATIONALE
➢ If a new application is required, consider the following options, in this order: • Reuse an existing application • Procure a prebuilt application, deployed in the cloud or on-premises. • Commission the creation of a new application	The scale and number of the University's IT project plans means that we must prioritise the time of our application development specialists to ensure they are available to work on strategic and innovative initiatives where no off-the-shelf solution exists. Note that existing applications should only be reused if they require little or no modification.
➢ Engage with IT business analysts to help with application proposals and business cases	Information Technology Services has a number of business analysts available to help document and understand your IT business requirements, prior to any commitment to procure or design new applications.
➢ Application data and metadata is accessible	Applications must provide appropriate access to their data via APIs or export facilities etc. Metadata must be available to aid re-use and aggregation of data for reporting and analysis.
➢ Applications are written using market leading tools & languages, including open source toolsets, and support open standards where practicable	We need to ensure that applications are easily supported and modified at the lowest cost. Application development skillsets and toolsets must also encompass those used in research (for example Java, Python, PHP, 'R')
➢ Applications run on Information Technology Services infrastructure & storage, or those of our approved cloud suppliers	Where applicable, ensure that applications can run easily on the platforms that the University of Otago already supports and for which service agreements are in place.
➢ Applications are demonstrably secure by design	Developers and vendors must build with security best practices in mind and be able to provide evidence to this effect. Application security measures must not unduly compromise user experience.
➢ Applications are clearly documented and must include solution architecture diagrams	Providing good documentation ensures that applications are well understood and supported throughout their lifetime.
➢ Applications or services utilising artificial intelligence, machine learning, deep learning and similar technologies must be carefully evaluated	The University encourages the use of these types of technologies, but the way they work, the training data sets they use, the biases they may contain, and their potential impact on our people must be carefully understood. IT staff to consult: *AI Adoption Principles for Tertiary Education*

Research IT

EA STANDARDS: RESEARCH IT	RATIONALE
➢ Identity and propose new shared, research IT services that can be made available University wide	It is more cost effective and efficient to share common research IT services where practicable. Information Technology Services will put forward proposals for additional services where there is sufficient demand, academic support and funding.
➢ Research IT infrastructure is used to provide research IT services	Research IT infrastructure is used to directly support research. It is not used to provide the common IT services that Information Technology Services already provide elsewhere (e.g. email, DNS, file serving, virtual servers, storage, business applications).
➢ Use research IT services provided by University of Otago funded partner organisations where practicable	Information Technology Services work with several University funded national eResearch organisations, for example the New Zealand eScience Infrastructure (NeSI), and the Research and Education Network New Zealand (REANNZ). NeSI provide high performance compute, data visualisation, storage and support services, and REANNZ provide research network and identity services. Information Technology Services have research focused IT specialists, and NeSI support specialists on campus. The University may partner with additional research IT provider organisations in the future, in collaboration with the University of Otago research community.
➢ Research IT infrastructure procurements should be made in consultation with Information Technology Services	It is advantageous if Information Technology Services specialists are involved in research IT infrastructure projects and procurement processes.
➢ Research IT infrastructure should be supported by Information Technology Services staff where practicable.	Information Technology Services may be able to help provide support for research IT services.

Data

EA STANDARDS: DATA	RATIONALE
➢ Data is an asset and is maintained and protected throughout its lifecycle	Ensure that data is stored securely, that its integrity, location and recoverability is known and tested, and that it remains accessible and reusable for those that need it. If possible, any available data definitions, descriptions and associated metadata are stored alongside source data. University data is only stored on University owned or approved systems and on Information Technology Services approved third-party services. Staff do not own University data but may act as data custodians or stewards on behalf of the University for particular data sets or domains. In this regard staff are responsible for controlling access to data, maintaining any associated metadata, and ensuring data quality, including the cleansing of older data.
➢ Primary data sources and data provenance is identifiable, and data is discoverable as appropriate	Primary data sources (where data is first created) are readily identifiable, and in the longer term will be stored in a central data register. For administrative systems primary data sources are typically an agreed 'single-source-of-truth' within a given domain. If primary data is subsequently imported into other unrelated systems, the provenance of that data is made obvious and is documented. The approval of the primary data source's custodian is obtained before it is reused.
➢ Where appropriate, data is potentially available to business intelligence, data analytics, AI, data mining and machine learning IT services that are approved by the University	Data is stored and described in a way that allows it to be reused within analytics and Business Intelligence solutions where appropriate. Expert advice is obtained prior to data being reused in this way, especially with respect to AI, machine learning, and deep learning (see: *AI Adoption Principles for Tertiary Education*).
➢ A common University wide data model is supported	As part of new IT services procurement & implementation projects, teams should make their service's data model and metadata available for inclusion into the University common data model repository, in the longer term.
➢ The meaning of data is clearly understood and managed	If the meaning of data changes over time, the University common data model repository is updated to reflect the change (in the longer term). Data fields within applications are used for the originally intended purpose unless there is broad agreement and planning for a change.

EA STANDARDS: DATA	RATIONALE
➢ Use of University data complies with University regulations, policies and applicable national and international legislation	Please consult with IT Assurance & Cybersecurity if you are unsure. Legislation that may apply when considering use of University data includes: The Privacy Act 1993 Health Information Privacy Code 1994, Public Records Act 2005, Copyright Act 1994.
➢ University data on mobile devices is protected	Ensure that appropriate and adequate data protection is in place on mobile devices (including laptops), and that highly sensitive data is not stored on the device at all. Mobile devices must be protected by an authentication challenge; where possible the storage media should be encrypted, and the device should have location services enabled and have remote wiping technologies enabled. Install and use the University VPN software on the device if you are concerned that your off-campus communications could be intercepted. Use multi-factor authentication if available.

IT Services Reuse

EA STANDARDS: SERVICES REUSE	RATIONALE
➢ IT services are flexible and configurable	When procuring or building IT services consider the University as a whole. How might others be able to use your service. If coding a new service, strive for loosely-coupled components that abstract out data, middleware, web and API functionalities.
➢ When designing or implementing large IT services, combine small modules that are relatively independent.	Prefer modular, microservice-based applications and services, that support open-standards, and possess resilient interfaces and APIs. All modules should support independent regression testing.

Identity

EA STANDARDS: IDENTITY	RATIONALE
➢ Use University identity authentication and authorisation services	The University has an Identity Management System that provides authentication and authorisation services. New capabilities such as multi-factor authentication and ORCID integration will be added to these core services. Bespoke or third-party authentication and authorisation services must not be used without prior approval from Information Technology Services. If all other factors are equal prefer to use Active Directory Federation Services, and Eduroam and Tuakiri federation.
➢ The University will consolidate its Active Directory infrastructures to a single secure domain, provisioned via the identity management system	As we adopt more cloud and federation services over time we need a single authoritative Windows Active Directory domain. Identity Management must not be a barrier to collaboration between staff and students.
➢ University owned devices use University authentication services for user logins, and are joined to the University Active Directory domain	Over time the University will adopt standard operating environments for Windows, Apple and Linux based devices; as a prerequisite these devices need to use a common set of management tools and authentication mechanisms. This will provide for greater agility, ease of future cloud adoption and security.
➢ University credentials are never copied, shared or repurposed for use within other applications or services	University usernames and passwords must not be reused, shared or stored, in applications or services that are not part of the Identity Management suite of services provided by Information Technology Services.
➢ A single University identity record per person is instituted, with multiple roles supported.	Over time changes will be made to the Central Identity Management Service such that there will be a single logical identity per person, while allowing more than one role to be associated with that identity (for example a person who is both a staff member and a student).
➢ University IT solutions using external cloud services, use the University's federated identity management services to authenticate users.	The University provides technologies to allow for the secure federation of University identity information with third parties.
➢ Users' identity management roles are clearly identified	Additional Identity roles provisioned for a person must reflect their actual roles in the organisation. Creating identity roles for any other purpose could compromise our services authorisation mechanisms and network security.
➢ A password vault is used to protect login credentials	We need to keep our role specific login credentials secure and backed up. Supported and approved password vault software that runs on our commonly used devices, will be made available soon. If you need a multi-user or role-based credentials vault, please contact Information Technology Services. Ensure that your manager has access to your University password vault.

EA STANDARDS: IDENTITY	RATIONALE
➢ Multi-factor authentication is to be provided as required	The University will make multi-factor authentication technology available as required. The University VPN service will use this technology, as will some Office 365 accounts.

Internal User Communications - Email, Instant Messaging, Mobile Devices

EA STANDARDS: INTERNAL USER COMMUNICATIONS	RATIONALE
➢ Use University provided email services and information	Information Technology Services provides a single email service that is available for all University users. Staff must not use third party email client services for University email (e.g. Gmail, iCloud)
➢ Use the University preferred instant messaging environments	Although a number of IT services provide instant messaging capabilities, work is underway to rationalise this situation and provide guidance to users. Current preferred environments include Slack, Zoom and Teams (in Office 365). Final recommendations will be made available soon via the *Register of Preferred University Services and Solutions.*

Glossary of Terms

CLOUD SERVICE
Is an information technology design pattern that provides pay-as-you-go access to third party, cloud based, IT infrastructure, platforms, and software. These environments are typically remote from the organisation that purchases them, they are subscription based, highly scalable, available on-demand, and are easily provisioned.

DATA PROVENANCE
Can be thought of as the history of a piece of data.

DEGRADE GRACEFULLY
The ability of an IT service to fail in a predictable, graduated way (as opposed to simply crashing). The service may still perform useful work while in a degraded state and may self-recover once the cause of the failure is resolved.

DEVICE
In computing terms this can mean a mobile phone, tablet, desktop, laptop, workstation, network, storage or compute component.

EDUROAM
Offers users from participating academic institutions secure Internet access at any other Eduroam participating location and uses federated identity services to authenticate and authorise access.

FEDERATED IDENTITY
The mechanism by which a person's digital identity is mapped and linked across a number of identity management systems belonging to other affiliated organisations.

FOG, EDGE AND MIST SERVICES
These are variants of a cloud service, that also place compute and storage at the edge of an organisation's network, as close as possible to the users' devices, to achieve better performance, lower latency and faster turnaround for particular types of time critical workloads.

HEADLESS DEVICE
Refers to a computing device that doesn't have a monitor, mouse or keyboard and / or graphical user interface software e.g. a printer or MRI scanner.

HYBRID CLOUD
A cloud service environment that uses both on-premise and public/private cloud third-party compute, storage, platform and software solutions, with an orchestration layer across them. This approach allows large organisations to make more strategic use of cloud services and is considered low risk and largely transparent to the organisation's user base.

IaaS | INFRASTRUCTURE AS A SERVICE
Is a type of cloud computing that provides for basic compute, storage, scaling, backup and security services. IaaS services are typically delivered over the internet but can be delivered on-premises as well.

IDENTITY AND ACCESS MANAGEMENT SYSTEM
A suite of software that manages users and devices on a network; may include functionality such as modelling user types and attributes, creating and disabling identity records, and authenticating or authorising user access to network resources.

IDENTITY BASED NETWORK
A network that is aware of user identities, and that uses this information to allow or deny access to parts of the network and to track users' activity on the network.

IT SERVICE
Using elements of information technology to deliver value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks.

LOOSELY-COUPLED APPLICATION
An application comprising relatively independent components that communicate via discoverable interfaces and publicly callable routines. These components should able to be tested or replaced with little impact to the rest of the application.

METADATA
Data that describes data. For example, a repository which describes published content metadata such as title and author, to enable users to locate items of interest. Metadata for a database system might include descriptions of every data field displayed by an application.

NeSI | NEW ZEALAND eSCIENCE INFRASTRUCTURE
Provides supercomputer, compute cluster, high speed storage, data analytics and data visualisation services to member research organisations. Also provides specialist staff to assist researchers.

ORCID
Is an international, unique identifier that researchers can use to prove their identity. The Orcid service also allows authorised publishers, funders and institutions to add supporting material to any given researcher's Orcid record.

PaaS | PLATFORM AS A SERVICE
Is a type of cloud computing that provides prebuilt services that serve a specific IT function. For example, a service that delivers a basic database server environment or that provides a LAMP stack for developers to use and customise. These services are typically delivered over the internet but can be delivered on-premises as well.

PACKAGE | PREBUILT, TESTED AND SUPPORTED SOFTWARE
Procured from a third party, that fulfils a business purpose. For example, a package designed to keep track of IT assets.

PATCHING
The process of updating previously installed software. Can also refer to the process of plugging network cables into a switch or similar device.

REANNZ
The Research and Education Network of New Zealand

SaaS | SOFTWARE AS A SERVICE
Is a type of cloud computing that provides prebuilt applications that serve a specific business purpose. For example, a service that delivers a library catalogue environment or that provides an HR system. These services are typically delivered over the internet but can be delivered on-premises as well.

TUAKIRI
A federated identity and authorisation service provided by REANNZ.

VPN SERVICE
Technology that tunnels encrypted network traffic from a private network, across a public network and into another network. For University of Otago staff this technology enables staff at home or around the globe to securely connect to the University network, as if they were on campus. Network traffic sent and received using this technology is difficult to intercept and is considered to be secure.