

Information Technology Standards and Guidelines

Version 2.0
January 2019



Information Technology Standards and Guidelines Version 2.0

© Government of Tasmania, 2019

Excerpts from this publication may be reproduced, with appropriate acknowledgment, as permitted under the Copyright Act.

For further information please contact:
Department of Treasury and Finance
GPO Box 147
Hobart Tasmania 7001
Telephone: +61 3 6166 4444
Website: www.treasury.tas.gov.au

Published January 2019

Contents

1	Introduction	4
1.1	About the Department.....	4
1.2	IT Service Delivery in the Department.....	4
1.3	Cloud-based ICT Services	4
1.4	Current IT Infrastructure.....	5
2	The Department's ICT Standards.....	7
2.1	User Interface Standards	7
2.2	ICT Security Standards.....	7
2.3	Architecture Standards	8
2.4	Information Technology Standards	8
2.4.1	Desktop Standards	8
2.4.2	Server Standards.....	9
2.4.3	Application Development Technology Standards.....	10
3	Application Design & Development Guidelines	12
3.1	Development Methodology	12
3.2	Implementation	12
3.3	Testing.....	12
3.4	Deployment.....	13
3.5	Documentation.....	13

1 Introduction

This document contains a summary of the overall Information Technology architecture and standards of the Department of Treasury and Finance Tasmania.

This document is intended to provide vendors and service providers with an understanding of the overall ICT architecture and standards of Treasury. It is also designed to be used in conjunction with tenders as supporting documentation.

1.1 About the Department

The Tasmanian Department of Treasury and Finance has overall responsibility for implementing strategies to achieve the Government's longer-term economic and financial objectives. It provides the Government with objective advice on the economic and financial management of the State; implements Government policy; performs financial analysis; monitoring and reporting functions on behalf of the Government; and supports statutory bodies responsible for administering State revenue collection and the regulation of gaming, liquor, energy and prices oversight.

As at 30 June 2018, the Department employed 311 full time equivalent people and its 2017-18 budgeted operating expenditure was \$69 million. The Department operates from the following main sites:

- Franklin Square (21 Murray St, Hobart).
- Salamanca Building, Parliament Square (4 Salamanca Place, Hobart).
- 21 Kirksway Place, Hobart.
- Henty House, Launceston.

1.2 IT Service Delivery in the Department

The Department's IT Services are provided by the Information Systems Branch (ISB) or third-party partners contracted by ISB. ISB is responsible for supporting and enabling the Department achieve better outcomes through the use of information technology and systems. This includes overseeing IT infrastructure and information system maintenance and support as well as IT architecture oversight and IT policy development and support. The branch is structured into three main units – Application Support, Infrastructure Support, and Information Management Projects. The Department's Corporate Information Support Branch provides records, communications, library and website management services.

1.3 Cloud-based ICT Services

The Department has a preference for selecting cloud-based services, including Software, Platform and Infrastructure as a Service, where the service provided represents the best value for money and adequate management of risk compared to other available options. The Department will consider all models of cloud based services, but aligned with the State Government [Tasmanian Cloud Policy](#) it

has a preference for Tasmanian-based Cloud services, where the services are delivered via “on-island” infrastructure.

1.4 Current IT Infrastructure

The Department provides all staff with access to a desktop computing device, with a laptops being the standard device issued.

The Department also supports all staff to use their own devices if they so desire (Bring Your Own Device, BYOD) and has a set of policies regarding the use of, and support for, BYO devices.

The following table describes the Department’s current IT infrastructure:

Hardware Component	Currently Deployed
Desktop computing device	<p>The Department uses Intel based desktop and laptop devices. The lowest specification devices deployed in the Department are i5-2400, 3.4GHz machines with 4GB RAM and 250GB HDDs.</p> <p>The minimum screen size is LCD 22”. Generally the Department has 23” wide-screen monitors and the resolution is set to 1920 x 1080, (though some users have a need for a higher or lower resolution).</p>
Mobile Devices	<p>Where there is a business requirement, the Department provides staff with a smartphone and or a tablet device.</p> <p>The Department uses Airwatch by VMWare for mobile device management on all Departmental supplied mobile devices.</p> <p>The Department additionally supports staff to use their own mobile devices if they so desire (Bring Your Own Device, BYOD).</p>
Printers & MFDs	<p>The Department has deployed Multi-Function Devices (MFDs) at central locations for shared use in printing, copying, scanning. Ricoh C4503SP devices are the current MFD devices in use. Secure print and release functionality has been implemented for these devices using Papercut. A few dedicated print devices have been deployed for specific purposes.</p>
Back-end infrastructure	<p>The Department has transitioned to using servers and storage provided under an Infrastructure as a Service (IaaS) model. These services are delivered from highly available data centres in Tasmania.</p> <p>The Department’s main sites each use layer 3 switches to support 1Gbps Ethernet LAN connections for the end users.</p> <p>The Department uses Microsoft based services (including directory, file and print, DNS, DHCP, proxy and database services). These services are all virtualised on the IaaS platform.</p> <p>The Department is also increasingly using Microsoft cloud based services including Skype for Business, SharePoint, Teams and One Drive for</p>

	Business.
--	------------------

2 The Department's ICT Standards

2.1 User Interface Standards

Web-based applications are strongly preferred. Such applications must be supported on, and run efficiently and effectively on, the Department's standard end user devices and standard Internet Browser (as in Section 2.4.1).

Unless otherwise agreed, all websites web-based applications must meet Web Content Accessibility Guidelines (WCAG) 2.0 level AA.

Additionally, any external / public-facing websites and web-based applications:

- must conform to the Tasmanian Government Website Standards (<http://www.communications.tas.gov.au/channels/websites>)
- where appropriate, conform to the Tasmanian Government Communications Policy (<http://www.communications.tas.gov.au/policy>)
- render appropriately and in a user friendly manner on a range of hardware devices including PCs, tablets and phones.
- support, and provide the same functionality in the following latest and recent versions of web browsers on major Windows, Mac and Linux, Android and iOS operating systems: Microsoft Edge, Internet Explorer, Google Chrome, Mozilla Firefox, and Safari.
- adopt the Department's website standard look and feel where practical (as decided by the Department).

2.2 ICT Security Standards

- All Treasury systems must conform with the [Whole of Government ICT Security Framework](#) including the [Whole of Government Information Security Policy Manual](#).
- The Tasmanian Government is currently developing an ICT Security Manual based on the ISO27002:2013 standard. All Treasury systems will be required to conform to this ICT Security Manual.
- Each application must be designed to meet the information and technical security requirements of the application and the Department. They must comply with the Information Security Charter and Guideline and Identity and Access Management Toolkit (www.egovernment.tas.gov.au/information_security_and_sharing).
- The Department prefers that applications integrate with Active Directory or Active Directory Federation Services (ADFS) for authentication and authorisation.
- Kerberos based integrated Authentication is preferred where the client is within the Treasury network, provided it meets the information security requirements of the application.
- Audit requirements, including Right to Information requests, archiving and retrieval requirements must be considered for each application. For most systems an audit trail is required - it is not sufficient to rely on the web server log files. It is preferred that the audit trail is in a database. Detailed audit requirements will depend on business need, including those of connected systems and services.

- Encryption of user credentials and sensitive information must be considered for each application.

2.3 Architecture Standards

- Where appropriate, applications must use an architecture that integrates with, and builds upon, a service-oriented architecture.
- Where appropriate, applications must be designed and developed in a modular fashion with reusable components.
- Application configuration and deployment settings must be easy to change (without the need to recompile code).
- The design of the application must consider the performance and, if appropriate, the scalability and extensibility of the application.
- The design of the application must consider the concurrency requirements and ensure the resulting system appropriately supports concurrent access.
- The design of the application must consider the availability and disaster recovery requirements for the application.

2.4 Information Technology Standards

This section presents the Department’s current Server, Desktop and Application Development technology standards respectively. As detailed in the notes column, for some technologies the Department currently uses multiple products, but has selected one product as its standard into the future. Generally, support and licensing arrangements will exist for the standard technologies.

Technology selection is a balance of several factors including business benefit, cost, supportability and maintainability. It is therefore possible that non-preferred technologies will be selected through the Department’s procurement processes. Such procurement processes may even cause the Department to revise its IT Strategy and associated technology standards.

2.4.1 Desktop Standards

Technology	Standard	Notes
Desktop Operating System	Windows 10 (64-bit)	Release 1709
Office Productivity Tools	Microsoft Office 2016 Word, Excel, PowerPoint.	Microsoft Access is not installed by default but is available based on business need.

Email Client	Microsoft Outlook Client 2016	The Department currently uses the Whole of State Government (Microsoft Exchange 2010) Email Service, with this scheduled to transition to email being provided from Office 365 within 3 months.
Web Browser	Microsoft Edge, Chrome, Internet Explorer 11	Flash and Java based applications will be blocked from running.
Other standard desktop software and settings	Adobe Reader DC Citrix Receiver Symantec Endpoint Protection (antivirus) HP Content Manager 9.1 Kapish add-ons for Outlook and Word Various desktop hardening settings following ASD recommendations	Staff do not have administrative privileges on the desktop device.

2.4.2 Server Standards

Important Note: the following standards are applicable for servers supported by the Department. As explained in the Introduction, the Department has a preference Software as Service provided via the Tasmanian Cloud where that service represents best value for money and adequate management of risk. Where Software is provided as a Service the Department is agnostic to the underlying server technology used.

Technology	Standard	Notes
Virtualisation	As provided by the IaaS supplier.	The current provider utilises VMware.

Server Operating System	Microsoft Windows Server Windows Server 2016 (64-bit).	
Database Management Software	Microsoft SQL Server 2016 running in an Always On Failover Cluster pair.	Because of the specialised expertise required around database administration and maintenance, an external supplier has been contracted to provide a Database Management as a Service (DBMaaS) to the Department. The Department WILL NOT use of Microsoft Access for mission critical systems and prefers not to use it even for single user databases that do not contain secure data.
Web Server	Microsoft IIS (version 10)	For new solutions, Software as a Service is strongly preferred.
Software Distribution, Imaging, Management and Monitoring Tools	Microsoft System Center	Current Branch is run where possible.

2.4.3 Application Development Technology Standards

Important Note: the following standards are applicable for software developed or maintained by the Department. Where Software is not supported or maintained by the Department, the Department is agnostic to the technology used.

Technology	Standard	Notes
------------	----------	-------

Development Environment	<p>Microsoft .Net with:</p> <ul style="list-style-type: none"> • Visual Studio 2017 • ASP.NET MVC version 5. (Versions 3 and 4 are also used and supported). • C# • ADO.NET Entity Framework 6 • Default ASPX view engine/Razor • jQuery • ASP.NET Master Pages, themes and CSS Style Sheets are used. 	<p>The Department also currently supports several Java Standard Edition 1.6x - based applications and a range of other technology, but has made a strategic decision to adopt .Net for new developments.</p>
Build Server and Version Control	Microsoft Team Foundation Server	<p>There is a planned upgrade to Azure Dev Ops in the next 12 months.</p> <p>Other build servers and version control systems are used for legacy technology.</p>
Release Management	Octopus Deploy	Manual release processes are used for legacy applications.

3 Application Design & Development Guidelines

Important Note: the following guidelines are applicable for software being specifically developed by, or on behalf of, the Department. They can also provide a useful guide to the Department's expectations when of vendors who provide commercial off-the-shelf and Software as a Service solutions to the Department.

3.1 Development Methodology

- The methodology used must allow for feedback from Treasury early in the development process and regularly throughout the development process.
- All development projects must have a project development plan that is approved by the Department before development begins. The plan should outline:
 - the development methodology;
 - the architecture, technology, security, and components / modules proposed;
 - procedures for reviewing and revising the development plan; and
 - the schedule of deliverables.
- Treasury strongly encourages automated build servers and continuous integration.

3.2 Implementation

- Applications must be developed according to a well-defined version management scheme (this should include versioning of the database and web service schemas where appropriate).
- Each version of the application released for testing, training, or to production must include the following artefacts in a logical and easy to navigate directory structure:
 - all source code that is or will be owned by Treasury;
 - all third-party libraries (possibly in binary format) and documentation for those libraries;
 - all build, install, test, and database scripts and projects and associated documentation to allow a test or production release to be automatically built; and
 - all deployment, technical, and user documentation.
- All source code must be developed according to a well defined coding standard that prescribes sufficient source code comments to easily understand the code.
- Treasury encourages development using the products listed in the Department's Application Development Technology Standards (see previous section).

3.3 Testing

- Treasury and the vendor will agree on the level of testing to be performed by the vendor. This may include unit, functional, system, regression, load, stress, volume, security, failover and recovery, configuration, and database testing. The testing performed (test scripts) and test results must be documented in an agreed format.

- Treasury strongly encourages Test Driven Development and conformance to the principles enunciated by the International Software Testing Qualifications Board (ISQTB).

3.4 Deployment

- Each release of an application must include deployment instructions tailored specifically to the Treasury environment. These instructions must include procedures both for upgrade from a previous release and for complete deployment (eg for disaster recovery).
- A Change Request must be approved by the Information Systems Branch before each release is deployed to a Treasury Test, Training, or Production environment.

3.5 Documentation

- The level and format of user and training documentation required with each release of the application will be negotiated on a case-by-case basis.
- Each release of the application must be accompanied by up-to-date technical documentation. The level of documentation required will be negotiated on a case-by-case basis. At a minimum it must include:
 - a Change Log (for corrected bug references) and Release Notes for the software release;
 - an overview of the application and its scope, including an Application Context Diagram;
 - an overview of the architecture, including a System Architecture Diagram;
 - an overview of the database models (if databases are used), including an Entity Relationship Diagram; and
 - a description of network requirements, including IP port usage.
- The technical documentation may also include various UML models such as object, sequence and state models.
- Where an application will use a service provided by another application, the developer should understand the requirements of that service and, if required, request documentation from the Information Systems Branch before commencing design of the application.

Document acceptance and release notice

Build Status:

Version	Date	Author	Reason	Section
Draft	January 2011	Glenn Lewis	Initial Draft	All
Version 1.0	February 2011	Glenn Lewis	Updates following internal review	All
Version 1.1	July 2011	Glenn Lewis	Minor Updates	All
Version 1.2	July 2012	Glenn Lewis	Minor Updates	All
Version 1.3	April 2014	Glenn Lewis	Minor Updates	All
Version 1.4	March 2015	Glenn Lewis	Review and updates. Key updates include to the technology standards, addition of mobility / BYOD, and cloud and “as a service” sections.	All
Version 1.5	November 2015	Glenn Lewis	Review, updates and changes to layout and style	All
Version 2.0	January 2019	Rob Hidding	Update of all sections	All